Privacy Year in Review: Growing Problems with Spyware and Phishing, Judicial and Legislative Developments in Internet Governance, and the Impacts on Privacy

MATTHEW BIERLEIN & GREGORY SMITH*

ABSTRACT

This article reviews the major events and issues involving the Internet and the privacy of individuals that arose in 2004. Spyware issues were a growing concern, and the section on spyware focuses on the tensions amongst government regulation, including legislative solutions and current litigation, valid business practices, and burdens on software developers. Costs to consumers and business infrastructure in relation to spyware are also discussed. This article also analyzes the growth in phishing, which involves using email to commit fraud upon consumers. Many proposed solutions are still targeting spam in general and not the specific bad acts presented by phishing. Domain name registration is focused on in the Internet governance section, with specific attention to legislation that all but mandates accurate contact information in publicly accessible databases. Furthermore, as technology changes, consumer protections must adapt. Corporations will need to maintain vigilance with regard to their customers' personal information, because there is an ever-present threat to security. The section discussing contemporaneous monitoring of Internet activity examines the trend of Internet-based communications becoming both more popular and less protected. This article also analyzes state attempts to begin forcing businesses to enact and comply with privacy policies, which restrict the businesses' use of and access to data. Finally, the article discusses federal and state efforts to protect children who use the Internet.

I. INTRODUCTION

An article on privacy and the Internet, in any setting, is an ambitious undertaking. With continuous changes in technology and ubiquitous concerns about privacy, it would not be possible to create a

* The authors are J.D. candidates at The Ohio State University Moritz College of Law, class of 2006, Matt Bierlein, B.A., *cum laude*, College of Wooster, 2001. Gregory Smith, B.A., Harvard University, 1999.

multi-volume treatise on privacy and the Internet. The goals of this paper are not so lofty. It is the intention of this paper to discuss various events relating to privacy and the Internet in 2004. During the writing of this paper events continuously unfolded in some of the topics discussed, and there has been a conscious effort to limit references to events both before and after 2004, except to point out when an event lacks resolution. Further, given the magnitude of the Internet, it is impossible for any paper to address every event and topic relating to privacy and the Internet, even within a given year. Therefore, this paper is broken up into the following eight topics: spyware, spam, phishing & spoofing, Internet governance, fraud & wrongdoing, contemporaneous monitoring of Internet activity, access to stored records from Internet activity, and online protection of children.

Spyware is discussed in Part I and focuses on the tensions amongst government regulation, including legislative solutions and current litigation, valid business practices, and burdens on software developers. Part II examines the increasing cost of spam in terms of both business infrastructure and consumer fraud with an eye towards various solutions proposed by the legislative, administrative, and private sectors. In Part III, phishing, the dramatic increase in the use of email to commit fraud upon consumers, is analyzed. Many proposed solutions are still targeting spam in general and not the specific bad acts presented by phishing. Part IV, Internet governance, focuses on domain name registration, with specific attention to legislation that all but mandates accurate contact information in publicly accessible databases. In Part V, fraud & wrongdoing, the dichotomy between consumer protection and changing technology is discussed. Corporations will need to maintain vigilance with regard to their customers' personal information, because there is an ever-present threat to security. Part VI, contemporaneous monitoring of Internet activity, examines the trend where Internet-based communications are becoming both more popular and less protected. Access to stored records from Internet activity, Part VII, analyzes the push by states to force businesses to enact and comply with privacy policies, which restrict their use of and access to data. Part VIII, online protections for children, discusses federal and state efforts to protect children who use the Internet.

II. SPYWARE

Originally, spyware referred to "computer software that gathers and reports information about a computer user without the user's

knowledge or consent."[1] With the increased interest from non-technical sources and a technical blurring of boundaries, the term "spyware" has come to encompass several subcategories, including spyware, adware, and malware.[2] For example, adware might install as spyware on a computer, running in the background and collecting information on the user's activities without his knowledge or consent. Then the program might display some form of comparative advertising at an appropriate time. Similarly, malware might install as spyware on a computer, running in the background, collecting information on the user's activities without his knowledge or consent, and negatively affecting the computer system in some way. For the purposes of this paper, the generic term spyware will be used to refer to all spyware, adware, and malware.

Notwithstanding the concerns about spyware infringing on a user's privacy by surreptitiously monitoring and reporting activity, spyware incurs a cost to the end user both in terms of time and money. Near the beginning of 2004, a leading Internet security company, McAfee Security, reported that spyware accounted "for over half of the top 20 malicious threats reported to [it]."[3] Further, it reported on a study performed by the National Cyber Security Alliance, which found that "91 percent of all home PCs are infected with some kind of spyware today."[4] In another study, EarthLink, an Internet Service Provider, found that "[t]he average computer [has an average of 28] hidden software [programs] that can secretly spy on online habits."[5] When viewed together, this means that 91% of all home PCs have, on

---

[1] *Spyware*, WIKIPEDIA, *at* http://en.wikipedia.org/wiki/Spyware (last visited March 11, 2005) (the definition used in this paper ignores another version of spyware: hardware-based devices that enable monitoring and reporting of activity through physical attachment to a computer.) [hereinafter WIKI SPYWARE].

[2] *Id. See also Adware*, WIKIPEDIA, *at* http://en.wikipedia.org/wiki/Adware (last visited March 11, 2005) (defining adware as "any software application in which advertisements are displayed while the program is running"); *see also Malware*, WIKIPEDIA, *at* http://en.wikipedia.org/wiki/Malware (last visited May 10, 2005) (defining malware as "any software program developed for the purpose of causing harm to a computer system").

[3] *Network Associates Introduces McAfee AntiSpyware - Essential Protection Against Spyware for Consumers*, HELP NET SECURITY (February 12, 2004)(capitalization changed throughout), *at* http://www.net-security.org/press.php?id=1973.

[4] *Id.*

[5] *PCs 'infested' with spy programs*, BRITISH BROADCASTING COMPANY (April 16, 2004), *at* http://news.bbc.co.uk/2/hi/technology/3633167.stm.

average, 28 hidden software programs surreptitiously collecting information on the user's activity.

It is difficult to quantify the cost of having spyware installed on these computers, because it is not releasing a payload or self-replicating as a virus would but is merely using computer resources. Still, some groups have tried to quantify this cost. For instance, "[a]s of 2004, spyware infection causes more visits to professional computer repairers than any other single cause."[6] Further, "[i]n more than half of these cases, the user has no awareness of spyware and initially assumes that the system performance, stability, and/or connectivity issues relate to hardware, Windows installation problems, or a virus."[7] One possible solution in lieu of going to a professional computer repairer is to perform "a clean install," where the computer's hard drive is completely erased, all essential software is reinstalled, and all files that were backed up are restored.[8] In an attempt to quantify these costs, PCX Technologies cited a Trend Micro study reporting that "in 2001 viruses, worm and spyware [sic] cost businesses $13 billion, in 2002 the cost rose to $20 - $30 billion and in 2003 viruses, worms and spyware cost a record $55 billion in damages."[9] Although these numbers are provided by vendors selling security products, and although the numbers include viruses along with spyware, there are clear costs associated with surreptitious programs running on a computer.

Given the explosive impact of spyware on the average consumer, there was increased attention given to spyware in 2004 from federal, state, and international governments to individuals and companies. The battle typically fought in both the legislative and judicial settings concerned the definition of spyware, with interested parties lobbying for either a more restrictive definition, thereby allowing certain forms of spyware to remain legal, or a more expansive definition, which would drastically restrict the use of spyware.[10]

---

[6] WIKI SPYWARE, *supra* note 1.

[7] *Id.*

[8] *Id.*

[9] *Services - Viruses • worms • spyware • adware*, PCX TECHNOLOGIES, *at* http://www.pcx.net/malware.htm (last visited March 17, 2005).

[10] *See, e.g.*, David Worthington, *AOL Answers Privacy Concerns in AIM Beta*, BETANEWS (April 16, 2004) (Discussing how a "[p]rior production releases of AIM drew criticism for forcibly installing Wild Tangent's gaming technology, which some privacy advocates consider to be spyware."), *at* http://www.betanews.com/article/1082143843.

A. FEDERAL LEGISLATION

The 108th Congress considered two types of bills concerning spyware: those that targeted bad acts, such as surreptitiously monitoring and reporting usage, and those that sought to define spyware, such that software fitting into the definition was brought under the auspices of the bill. None were enacted, however.

One example of a bill that targeted bad acts was the I-SPY Act of 2004, which included Congressional findings stating that "[s]oftware and electronic communications are increasingly being used by criminals to invade individuals' and businesses' computers without authorization ... to obtain personal information, such as bank account and credit card numbers, which can then be used as a means to commit other types of theft."[11] The bill sets out specific bad acts, stating that:

> [w]hoever intentionally accesses a protected computer ... by causing a computer program ... to be copied onto the protected computer, and intentionally uses that program [to further] another Federal criminal offense[;] ... [to] obtain[], or transmit[] to another, personal information with the intent to defraud or injure a person or cause damage to a protected computer; or ... [to] impair[] the security protection of the protected computer

has engaged in illegal conduct.[12]

On the other hand, the SPY ACT of 2004 tried to define spyware in order to mandate that the spyware program provide notice of its presence and receive consent before its installation.[13] Because lack of notice and consent upon installation are seminal in defining spyware,

---

[11] Internet Spyware (I-SPY) Prevention Act of 2004, H.R. 4661, 108th Cong. (2004) (as received in the Senate from the House), *available at* http://thomas.loc.gov/cgi-bin/query/z?c108:H.R.4661: (last visited March 11, 2005) [hereinafter I-SPY ACT]. This bill has been reintroduced to the 109th Congress as H.R. 744, 109th Cong. (2005), *available at* http://thomas.loc.gov/cgi-bin/bdquery/z?d109:H.R.744: (last visited March 11, 2005).

[12] *Id.*

[13] Securely Protect Yourself Against Cyber Trespass Act (SPY ACT) of 2004, H.R. 2929, 108th Cong. (2004) (as received in the Senate from the House), *available at* http://thomas.loc.gov/cgi-bin/query/z?c108:H.R.2929: (last visited March 11, 2005) [hereinafter SPY ACT]. This bill has been reintroduced to the 109th Congress as H.R. 29, 109th Cong. (2005), *available at* http://thomas.loc.gov/cgi-bin/bdquery/z?d109:H.R.29: (last visited March 11, 2005).

requiring notice and consent is a technical solution that will remove software from the category of spyware and likely provide the ability for legal relief, should the software exceed its consented use.[14] Practically however, there may be some unintended consequences of a strict notice and consent requirement for software. First, one must define exactly which software is required to provide notice and receive consent. Second, one must establish some *de minimis* standard for notice and consent. Finally, the definitions and standards must balance consumer concerns over spyware with the compliance burden placed on legitimate software manufacturers.

The SPY ACT defines an "information collection program" as the type of program required to provide notice and receive consent, seemingly addressing the concerns of spyware surreptitiously monitoring a computer user's activity.[15] The Act goes on to define an information collection program as two different types of program, the first of which is computer software that "collects personally identifiable information; and ... sends such information to a person other than the owner or authorized user of the computer, or ... uses such information to deliver advertising to, or display advertising, on the computer."[16] The second type of information collection program is computer software that "collects information regarding the Web pages accessed using the computer; and ... uses such information to deliver advertising to, or display advertising on, the computer."[17] Because many different types of software collect personally identifiable information and transmit it to third parties, such as the registration wizard typically found in many software installation packages, this

---

[14] *See* WIKI SPYWARE, *supra* note 1.

[15] SPY ACT, *supra* note 13.

[16] *Id.*

[17] *Id.* There is an exception in the definition of "computer software" for cookies, which it defines as any "text or data file that is placed on the computer system of a user ... to return information to ... or ... to enable the user subsequently to use such provider or service or to access such website." *Id. See also HTTP Cookie*, WIKIPEDIA *at* http://en.wikipedia.org/wiki/HTTP_cookie (last visited March 12, 2005) (defining a cookie as a small text file that may be stored on the user's computer after accessing a web site. The use of cookies varies with some being "used to authenticate or identify a registered user of a web site as part of their first login process or initial site registration without requiring them to sign in again every time they access that site" while others are used for "maintaining a 'shopping basket' of goods selected for purchase during a session at a site, site personalisation [sic] (presenting different pages to different users), and tracking a particular user's access to a site.").

definition is broad.[18] A broad definition does not necessarily burden software developers, however, as long as the notice and consent standards are malleable.

The SPY ACT establishes *de minimis* standards for notice and consent, calling for "clear and conspicuous notice in plain language" that is subject to the following inclusive requirements:

> 1) that the "notice *clearly distinguishes such notice* from any other information visually presented contemporaneously on the protected computer;"
>
> 2) that the "notice *contains one of the following statements*, as applicable, or a substantially similar statement," with three model notices described in the bill;
>
> 3) that the *lack of consent* to the notice *terminates the transmission* of the information;
>
> 4) that the "notice provides an *option* for the user to select *to display ... a clear description* of ... the *types of information to be collected and sent* ... [and] the *purpose* for which such information is to be collected and sent;" *and*
>
> 5) that the "notice *provides for concurrent display of the information required* ... until the user" consents to or declines the options presented in the notice.[19]

These requirements clearly establish standards for notice and consent, but they do not balance the consumer concerns over spyware with the compliance burden placed on legitimate software manufacturers.

By establishing such granular requirements, the bill would dictate software design requirements for all software manufactures that collect information, from Microsoft to the part-time software developer working out of her garage. For example, the requirement of concurrent display would necessitate changes in a variety of existing software products and could be particularly challenging to implement,

---

[18] *See Wizard (software)*, WIKIPEDIA (defining a wizard as "an interactive computer program acting as an interface to lead a user through a complex task" using discrete steps), *at* http://en.wikipedia.org/wiki/Wizard_%28software%29 (last visited on March 12, 2005).

[19] SPY ACT, *supra* note 13 (emphasis added).

depending on the software development environment and a plethora of other variables. Further, there are other requirements, such as that the software manufacturer "shall provide another notice in accordance with this subsection and obtain consent before such program may be used to collect or send information of a type or for a purpose that is materially different from, and outside the scope of, the type or purpose set forth in the initial or any previous notice."[20] This requirement dictates that the software manufacturer must build in functionality to contact the user proactively, should any of the information collection routines of the computer software change. For example, if a user downloads the latest update to his computer software and that patch transmits any information, the software manufacturer will have to develop a routine to interact with the user and obtain the user's consent. These additional requirements may be useful practices for a software manufacturer to undertake, but they will certainly add to the cost of developing and maintaining software. Finally, after the expense of complying with these requirements, users might treat the notice and consent provisions as they currently treat End User Licensing Agreements where "[u]sers almost invariably click on 'Accept' without reading the license."[21] Some of the disputes that may arise under this bill have already arisen under similar state legislation, with parties challenging whether their software falls under the definition of spyware.

The SPY ACT also included a section defining specific bad acts, although at a much more detailed and technical level than those defined in the I-SPY Act of 2004.[22] Without going into the minutia, SPY ACT targets the following bad acts:

> (1) *Taking control* of the computer....
>
> (2) *Modifying settings* related to use of the computer or to the computer's access to or use of the Internet....
>
> (3) *Collecting personally identifiable information* through the use of a keystroke logging function.

---

[20] *Id.*

[21] *Software license*, WIKIPEDIA, *at* http://en.wikipedia.org/wiki/Eula (last visited March 11, 2005).

[22] *See* SPY ACT, *supra* note 13.

> (4) *Inducing* the owner or authorized user *to install a computer software component* onto the computer, or preventing reasonable efforts to block the installation or execution of, or to disable, a computer software component....
>
> (5) *Misrepresenting that installing a separate software component* or providing log-in and password information *is necessary* for security or privacy reasons, or that installing a separate software component is necessary to open, view, or play a particular type of content.
>
> (6) *Inducing* the owner or authorized user to install or execute computer software *by misrepresenting the identity or authority* of the person or entity providing the computer software to the owner or user.
>
> (7) *Inducing* the owner or authorized user *to provide personally identifiable, password, or account information* to another person....
>
> (8) *Removing, disabling, or rendering inoperative* a *security*, anti-spyware, or anti-virus technology installed on the computer.
>
> (9) Installing or executing on the computer one or more additional computer software components with the *intent of causing a person to use such components in a way that violates any other provision of this section*.[23]

Recalling the distinction between spyware, adware, and malware, the nine bad acts enumerated in SPY ACT canvas all three areas, including "taking control of the computer by ... delivering advertisements that a user of the computer cannot close."[24] Because of the specificity with which the bad acts are described, however, there is a reasonable argument under the maxim of *expressio unis est exclusio alterius* that acts falling outside of those enumerated are legal. In

---

[23] *Id.* (emphasis added).

[24] *Id.*

comparison, many of the same bad acts fall under the broader language of the I-SPY Act, which ensures continuous protection as new software and technologies emerge.[25]

Finally, the SPY ACT explicitly preempts state spyware laws, stating that "[t]his Act supersedes any provision of a statute, regulation, or rule of a State or political subdivision of a State that expressly regulates" bad acts, transmission of information without notice and consent, or "the use of computer software that displays advertising content based on the Web pages accessed using a computer."[26] Therefore, a brief discussion of state legislation is in order.

B. STATE LEGISLATION

Two states, Utah and California, enacted spyware legislation in 2004. Utah enacted the Spyware Control Act, which defines spyware in such a manner as to target adware specifically.[27] The Act states that spyware is software that "monitors the computer's usage" and either "sends information ... to a remote computer or server" or "displays or causes to be displayed an advertisement in response to the computer's usage if the advertisement" comes from or is triggered by the installed spyware or is otherwise secretive about its source.[28] The Utah law defines not only the categories of information but specific information, such as a user's contact information, that is protected by the law. It also establishes a private action for people or organizations who "are adversely affected by a violation of this chapter."[29] Finally, it requires notice and consent by defining spyware as something that "monitors the computer's usage" for information that it will use to perform an action without obtaining "the consent of the user" before performing said action.[30] The consent requirements are copious and detailed, requiring consent to five different items, including a "license agreement," "notice of the collection of each specific type of information," "a clear and representative full-size example of each

---

[25] *See* I-SPY ACT, *supra* note 11.

[26] SPY ACT, *supra* note 13.

[27] *Spyware Control Act*, UTAH CODE ANN. §§ 13-40-101 to 401 (2004).

[28] § 13-40-102 (2004).

[29] *Id.*; § 13-40-301(b).

[30] § 13-40-102.

type of advertisement," "truthful statement of the frequency" of the advertisements, and "a clear description of a method by which a user may distinguish the advertisement ... from an advertisement generated by other software services."[31] Specific instances of litigation under this law are discussed in the state litigation section, below.[32]

California enacted the Consumer Protection Against Computer Spyware Act, which targets the broader category of spyware, including adware and malware.[33] The statute defines specific bad acts, including, for example, modifying, "through intentionally deceptive means ... [certain] settings related to the computer's access to, or use of, the Internet;" collecting, "through intentionally deceptive means, personally identifiable information;" and "[t]hrough intentionally deceptive means, remov[ing], disabl[ing], or render[ing] inoperative security, antispyware, or antivirus software installed on the computer."[34] Further, the Act defines "intentionally deceptive" as 1) an "intentionally and materially false or fraudulent statement," 2) a "statement or description that intentionally omits or misrepresents material information in order to deceive the consumer," or 3) an "intentional and material *failure to provide any notice* to an authorized user regarding the download or installation of software in order to deceive the consumer."[35]

The Utah and California laws have some similarities and some differences. Both define spyware and bad acts, but they do not define them in the same manner. This legal disparity has the potential to disadvantage the software manufacturers, who will have to develop their products to comply with the most restrictive provisions of all state laws, if they want to distribute their software in more than one state, provided the state laws do not conflict with each other. Perhaps it is appropriate that both the Utah and California laws would be

---

[31] *Id.*

[32] *See, e.g.*, WhenU.com, Inc. v. State, Case No. 040907578 (3d Judicial Dist. Ct. Utah June 22, 2004) (preliminary injunction enjoining Utah from enforcing the *Spyware Control Act*, pending a decision on its constitutionality), *at* http://www.siia.net/govt/docs/pub/SLC-306350-v1-Preliminary%20Injunction%20-%20WhenU.Com%20v.%20State.pdf.

[33] CAL. BUS. & PROF. CODE §§ 22947 - 22947.6 (2004) (effective January 1, 2005).

[34] § 22947.2.

[35] § 22947.1 (emphasis added).

explicitly preempted if the Federal SPY ACT bill is enacted, providing at least clear direction to software manufacturers.[36]

C. INTERNATIONAL LEGISLATION

Before discussing litigation that has arisen concerning spyware, there was at least one international development relating to spyware in 2004 in Australia.[37] Senator Brian Greig sponsored a bill that would not "ban anything" but would "[merely] seek[] to ensure openness and honesty."[38] Greig's statement went on to say that "[n]o program or cookie or any other form of tracking device is to be installed on any computer without the user of that computer being given clear information as to the purpose of the program or tracking device."[39] Greig advocates targeting a broader category of spyware, including adware and malware, in that "the bill will cover malware which includes viruses, trojans, and worms that 'all have the ability to cause loss of data or allow someone else to control your machine'.[sic]"[40] The proposed bill identifies specific bad acts, such as "key stroke loggers and screen capture utilities used to capture passwords, adware designed to deliver targeted advertising, and 'the annoying' which covers pop-ups, pop-unders, and homepage reset programs."[41] Although Greig admits that "[i]t's not certain that [actions against] international companies can be enforced," this bill would create one more set of rules with which software manufacturers need comply.[42]

---

[36] SPY ACT, *supra* note 13.

[37] Rodney Gedda, *Nation's first spyware laws to go before Parliament*, COMPUTERWORLD (June 21, 2004), *at* http://www.computerworld.com.au/index.php/id;187186972;fp;16;fpid;0 [hereinafter GEDDA ARTICLE].

[38] *Id.* (quoting Senator Brian Greig). Senator Greig has been a Senator for Western Australia since 1999 and sponsored the legislation. More information on Senator Greig is available on his website, *at* http://www.briangreig.democrats.org.au/.

[39] GEDDA ARTICLE, *supra* note 37. It may be worth tangentially noting that Senator Greig's logic is technically flawed because even if a website requests permission to store a cookie, it could not remember that a user said, "no," without storing the cookie.

[40] *Id.* (quoting Senator Brian Greig).

[41] *Id.*

[42] *See id.*

D. FEDERAL LITIGATION

Federal litigants have brought complaints under various theories, including violation of federal and state copyright, trademark, and unfair competition laws, because Congress has yet to enact federal anti-spyware legislation. One such case is *1-800 Contacts Inc. v. WhenU.com Inc.*, where WhenU.com, the purveyor of the product SaveNow, and Vision Direct, a company who advertises through WhenU.com, were enjoined by the District Court from:

> 1) including the 1-800 Contacts mark, and confusingly similar terms, as elements in the SaveNow software directory, and
>
> 2) displaying [the 1-800 Contacts] mark "in the ... advertising of" ... Vision Direct's services, by causing ... Vision Direct's pop-up advertisements to appear when a computer user has made a specific choice to access or find [1-800 Contacts] website by typing [1-800 Contacts'] mark into the URL bar of a web browser or into an Internet search engine.[43]

Essentially, "when a user type[d] in '1800contacts.com,' ... the SaveNow software recognize[d] that the user [was] interested in the eye-care category, and retrieve[d] from an Internet server a pop-up advertisement from that category."[44] In this case, the pop-up advertisement was an advertisement for Vision Direct.[45] The court denied the copyright claims, basing much of its rationale on the policy that:

> [f]or this Court to hold that computer users are limited in their use of Plaintiff's website to viewing the website without any obstructing windows or programs would be to subject countless computer users and software developers to liability for copyright infringement and contributory

---

[43] 1-800 Contacts, Inc. v. WhenU.com, 309 F. Supp. 2d 467, 510 (S.D.N.Y. 2003), *appeal not docketed.*

[44] *Id.* at 476.

[45] *Id.*

> copyright infringement, since the modern computer environment in which Plaintiff's website exists allows users to obscure, cover, and change the appearance of browser windows containing Plaintiff's website.[46]

The court approved the injunction, however, finding that 1-800 Contacts might be meritorious on its trademark claim against WhenU.com because, "[h]aving established a likelihood of confusion, Plaintiff has established both a likelihood of success on the merits and irreparable harm on its trademark infringement claim."[47] Therefore, absent federal spyware legislation, there still appears to be legal theories that support a cause of action.[48] The case is currently on appeal to the Second Circuit.[49]

L.L. Bean, an on-line and catalog merchant, has been actively pursuing trademark violation claims by filing separate complaints against various companies who advertise through Claria, an adware provider.[50] Claria stands to have its business eroded if L.L. Bean is successful in suing its customers and has sued L.L. Bean, alleging that L.L. Bean has undertaken a "campaign to interfere with Claria's

---

[46] *Id.* at 485, 488.

[47] *Id.* at 504-05.

[48] The case is currently on appeal, with both Google and the Electronic Frontier Foundation ("EFF") each advocating reversal. *See Trademark Law Shouldn't Prejudice Internet Ads*, ELECTRONIC FRONTIER FOUNDATION (February 19, 2004), *at* http://www.eff.org/IP/TM/20040219_eff_pr.php; *see also Brief of Amicus Curiae Google Inc. Supporting Neither Appellants Nor Appellee but Supporting Reversal*, (February 18, 2004) (arguing that using text to trigger functionality is not the use considered under the trademark act), *available at* http://law.marquette.edu/goldman/ googleamicus1800contactsvwhenuappeal.pdf. Google's argument may be particularly important, considering that the Ninth Circuit has also held that a trial court could find that a search engine had committed trademark violations. The case was ultimately settled. *See Netscape, Playboy settle search trademark case, CNET.COM* (January 23, 2004), *at* http://news.com.com/2100-1024-5146502.html.

[49] *1-800 Contacts*, 309 F. Supp. 2d at 510.

[50] *See, e.g.*, L.L. Bean v. Atkins Nutritional, No. 04-0099 (D. Me 2004) (alleging trademark violation, among other claims, and seeking injunctive relief and damages against Atkins, a purveyor of pop-up advertisements through spyware, for "parasitic" placement of advertisements on L.L. Bean's website), *available at* http://www.gigalaw.com/library/llbean-atkins-complaint-2004-05-17.pdf (last visited March 12, 2005).

business relationships" through sham litigation and disparaging press releases.[51]

Other federal actions have included defenses that anti-spyware programs are protected as free speech by the First Amendment;[52] Federal Trade Commission actions against adware and spyware companies for using adware and spyware, respectively, to advertise their anti-adware and anti-spyware products;[53] and lawsuits by InternetAd Systems, a pop-up-ad company, seeking royalties from several media outlets, claiming infringement upon patents over pop-up-style advertisements.[54]

E. STATE LITIGATION

Another area of litigation has been in state courts. Much like federal courts, some litigation has taken place in the form of novel applications of existing law, such as state wiretap statutes. Additionally, however, litigation has been brought challenging Utah's Spyware Control Act, Utah Code Ann. §§ 13-40-101 to 401 (2004).

In a novel approach to litigating against spyware, a Florida case challenged spyware as an illegal interception under state wiretap laws.[55] This case was decided on appeal from a marriage dissolution proceeding in early 2005, where a "[h]usband contend[ed] that ... spyware installed on the computer acquired his electronic communications real-time as they were in transmission and, therefore, are intercept[ions] illegally obtained under the Act."[56] The court

---

[51] Claria v. L.L. Bean, No. 2-04CV-207(E.D. Tex 2004)(capitalization altered), *available at* http://www.gigalaw.com/library/claria-llbean-complaint-2004-06-03.pdf (last visited March 12, 2005).

[52] *See* New.Net, Inc. v. Lavasoft, 356 F. Supp. 2d 1090, 1096-97 (C.D. Cal. 2004).

[53] *See* FTC v. D Squared Solutions, No. 03-CV-3108 (D. Md. 2004); FTC v. Seismic Entertainment Prods, No. 04-377 2004 WL 2403124, at *1, *slip copy*, (D.N.H. 2004). For a general spyware overview from the FTC, see *Spyware Workshop: Monitoring Software on Your PC: Spyware, Adware, and Other Software*, FTC STAFF REPORT (March 2005), *available at* http://ftc.gov/os/2005/03/050307spywarerpt.pdf.

[54] Stefanie Olsen, *Patent owner stakes claim in Net ad suit* (January 7, 2004), *at* http://news.com.com/2100-1024_3-5136909.html; *see also* InternetAd Sys. v. ESPN Inc., No. 03-2787 (N.D. Tex. 2004).

[55] O'Brien v. O'Brien, 2005 WL 322367, at *4-5 (Dist. Ct. of Appeal of Fla., 5th Dist. Feb. 11, 2005), *available at* http://www.5dca.org/Opinions/Opin2005/020705/5D03-3484.pdf.

[56] *Id.* at *1.

concluded "that because the spyware installed by the [w]ife intercepted the electronic communication contemporaneously with transmission, copied it, and routed the copy to a file in the computer's hard drive, the electronic communications were intercepted in violation of the Florida Act."[57] This conclusion was notwithstanding "[t]he fact that the definition of 'wire communication' provides for electronic storage while the definition of 'electronic communication' does not, suggest[ing] to the federal courts that Congress intended 'intercept' to include retrieval from storage of wire communications, but exclude retrieval from storage of electronic communications."[58] Therefore, the court of appeals affirmed the trial court's decision to exclude the communications from evidence.[59]

In another case, WhenU.com, a defendant in the *1-800 Contacts* case discussed under Federal Litigation, *supra*, challenged the constitutionality of Utah's Spyware Control Act on the grounds that the company would suffer irreparable injury.[60] After an initial hearing, the Court determined:

> that [WhenU.com would suffer] irreparable injury unless the requested preliminary injunction is issued, ... that preliminary injunction requested by Plaintiff is not adverse to the public interest, ... [and] that as to portions of the Utah Spyware Control Act there is a substantial likelihood that [WhenU.com] will succeed on the merits of its constitutional claims....[61]

Therefore, the court issued the preliminary injunction, preventing Utah "from enforcing or placing into effect the Utah Spyware Control

---

[57] *Id.* at *3.

[58] *Id.* at *4.

[59] *Id.* at *5.

[60] *WhenU.com, Inc. v. State*, *supra* note 32.

[61] *Id.*at 2.

Act."[62] Other litigants are currently waiting to find out if the lawsuits they filed under the Spyware Control Act will go forward.[63]

F. CONCLUSION

The services offered by some spyware programs, such as context-sensitive comparative marketing, are not inherently bad. For example, most consumers likely do not complain when search engines display targeted banner advertisements as a result of the search criteria entered. The concern comes from the surreptitious information gathering, storing, and transmission that is associated with the broader category of spyware rather than merely with adware. With spyware becoming an increasingly popular topic, legislatures may be feeling the pressure from their constituents to act, and some have acted with varied results. Comparatively, others "would like to see a more serious effort made to use existing laws against unfair trade practices, misrepresentation, computer fraud and abuse, before new technology-specific laws are passed."[64] Either way, the balance of public versus private interests will need to be struck in such a manner as to protect consumer privacy while permitting legitimate advertising services and not overburdening software manufacturers.

II. SPAM

Spam, or unsolicited commercial email ("UCE"), is the process by which identical or nearly identical messages are sent to multiple recipients without the recipient's permission.[65] Because these emails are sent without consumer consent, spammers use a variety of different means to acquire consumers' email addresses. Spammers may use email addresses that have been published online for other purposes, such as Usenet posts, corporate directories, or discussion groups; they may engage in dictionary attacks, generating likely email addresses from common names; or they may resort to even more surreptitious

---

[62] *Id.*

[63] *See, e.g.*, Janis Mara and Ron Miller, *Lawsuit Filed Under Utah's Challenged Anti-Spyware Act*, INTERNETNEWS.COM (May 19, 2004), *available at* http://www.internetnews.com/ec-news/article.php/3356441.

[64] GEDDA ARTICLE, *supra* note 37 (stating the view of the Electronic Frontier Foundation).

[65] *E-mail Spam*, WIKIPEDIA *at* http://en.wikipedia.org/wiki/E-mail_spam (last visited Feb. 17, 2005).

means, such as including code in a spam message that relays users' email or addresses book to the spammer's site.[66]

The economic costs of spam are substantial. While an exact number is difficult to ascertain, the cost of spam in the United States is estimated to be between $10 billion and $87 billion dollars.[67] These estimates cover a wide range of factors, including impact on worker productivity, infrastructure cost for spam filtering, and handling complaints.[68] In contrast, the cost to the spammer is minimal, sometimes as little as .025 cents per email.[69] In essence, the cost of spam is shifted from the commercial emailer to the Internet Service Providers ("ISP"), who send and receive the email, as well as to email recipients.[70]

The pernicious nature of spam has met with a strong legislative response. In December of 2003, Congress passed the CAN-SPAM Act of 2003.[71] The law prohibits both the false or misleading transmission of information and the use of deceptive subject headings.[72] It requires that UCE contain a valid return email address and a method by which consumers may opt-out of receiving email from certain spammers.[73] Additionally, UCE must contain clear and conspicuous identification that the transmitted message is an advertisement or solicitation.[74] A violation of the provisions of CAN-SPAM is treated as an unfair or deceptive act or practice and is primarily enforced by the Federal

---

[66] *Id.*

[67] Saul Hansell, *Totaling Up the Bill for Spam*, N.Y. TIMES, July 28, 2003, at C2.

[68] *Id.*

[69] Erin E. Marks, Note, *Spammers Clog In-boxes Everywhere: Will the CAN-Spam Act of 2003 Halt the Invasion?*, 54 CASE W. RES. L. REV. 943, 944 (2004); *see also* Dominique-Chantale Alepin, Note, *"Opting-Out": A Technical, Legal and Practical Look at the CAN-Spam Act of 2003*, 28 COLUM.-VLA J.L. & ARTS 41, 48 (2004).

[70] Marks, *supra* note 69, at 945.

[71] Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (codified at 15 U.S.C. § 7701-7713, 18 U.S.C. §1037, 28 U.S.C. § 994 (2003)).

[72] 15 U.S.C. § 7704(a)(1), (a)(2).

[73] § 7704(a)(3)–(5).

[74] § 7704(a)(5)(A)(i).

Trade Commission ("FTC").[75] CAN-SPAM gives other federal agencies certain enforcement powers, and also empowers state attorneys general and ISPs with the right to bring civil actions in particular circumstances.[76] The efficacy of CAN-SPAM has been widely debated with criticism that the Act has essentially legalized spam.[77]

In addition to federal legislation, thirty six states have enacted laws directed against spam.[78] Although these laws vary from state to state, there are some common themes. Most states establish definitions differentiating commercial email and UCE.[79] Many states have a labeling requirement mandating that UCE contain particular characters in the subject line.[80] Most state laws also contain an opt-out requirement for spam.[81] Some state legislation directly regulates

---

[75] § 7706(a).

[76] § 7706(f), (g).

[77] Marks, *supra* note 69, at 952; Adam Mossoff, *Spam – Oy, What a Nuisance!*, 19 BERKELEY TECH. L.J. 625, 636 (2004).

[78] ALASKA STAT. § 45.50.479 (Michie 2004); ARIZ. REV. STAT. § 44-1372 (2004); ARK. CODE ANN. § 4-88-601-607, 5-41-201-206 (Michie 2004); CAL. BUS. & PROF. CODE § 17529, 17538.45 (West 2004); COLO. REV. STAT. § 6-2.5 (2004); CONN. GEN. STAT. § 53-451- 453, 52-59b (2004); DEL. CODE. ANN. tit. 11, § 931-938 (2004); FLA. STAT. CH. 668.60 (2004); IDAHO CODE § 48-603E (Michie 2004); 815 ILL. COMP. STAT. 511/1-/15 (2004), 720 ILL. COMP. STAT. 5/16D-3 (2004); IND. CODE § 24-5-22 (2004); IOWA CODE § 714E.1, 714E.2 (2004); KAN. STAT. ANN. § 50-6,107 (2004); LA. REV. STAT. ANN. § 73.1, 73.6 (West 2004); ME. REV. STAT. ANN. tit. 10, § 1497 (West 2004); MD. CODE ANN., COM. LAW § 14-3001-3003 (2004); MD. CODE ANN., CRIM. LAW § 3-805-805.1 (2004); MICH. COMP. LAWS § 752.1061- .1068 (2004); MO. REV. STAT. § 407.1123, .1126, .1129, .1132 (2004); NEV. REV. STAT. 205.492, .511-.513, 41.705-.735 (2004); N.M. STAT. ANN. § 57-12-23, -24 (2004); N.C. GEN. STAT. § 14-453, -458 (2004); N.D. CENT. CODE § 51-27-01 (2004); OHIO REV. CODE ANN. § 2307.64 (2004); OKLA. STAT. tit. 15, § 776.1-776.6 (2004); OR. REV. STAT. § 646.607 (2004); 18 PA. CONS. STAT. § 5903 (2004); R.I. GEN. LAWS § 6-47-2, 11-52-1- 6 (2004); S.D. CODIFIED LAWS § 37-24-37- 40 (Michie 2004); TENN. CODE ANN. § 47-18-2501, 2502 (2004); TEX. BUS. & COM. CODE ANN. § 46.001-.011 (Vernon 2004); UTAH CODE ANN. § 13-39-101- 102, -201 (Effective July 1, 2005); VA. CODE ANN. § 18.2-152.4, 152.12, 152.3C1 (Michie 2004); WASH. REV. CODE § 19.190.010 - .050 (2004); W. VA. CODE § 46A-6G1- 6G5 (2004); WIS. STAT. § 944.25 (2004); WYO. STAT. ANN. § 40-12-401-404 (Michie 2004); *see also* http://www.ncsl.org/programs/lis/legislation/spamlaws02.htm (last visited Feb. 18, 2005).

[79] Jordan M. Blanke, *Canned Spam: New State and Federal Legislation Attempts to Put a Lid On It*, 7 COMP. L. REV. & TECH. J. 305, 307-08 (2004).

[80] *Id.*

[81] *Id.* (At present, California is the only state which has approved an opt-in requirement).

particular spammer conduct and spam content in an effort to protect consumers.[82] With regard to punishing illegal spamming, some states provide both misdemeanor and felony sanctions, while others sanction spamming as only a misdemeanor offense.[83] In addition to criminal penalties, many states allow for the commencement of civil actions.[84]

Two critical issues regarding state spam legislation are preemption and jurisdiction. CAN-SPAM preempts all state laws that specifically regulate UCE.[85] CAN-SPAM permits state legislation which prohibits false and deceptive UCE; however, the preemption provision may render many state laws ineffective.[86] An additional concern is that state anti-spam laws may affect commerce not entirely within the state and thus be unconstitutional by way of the dormant Commerce Clause.[87]

A. FEDERAL ADMINISTRATIVE DEVELOPMENTS

In 2004, the FTC promulgated a new rule regarding sexually explicit email. Section 7704(d) of CAN-SPAM required the FTC to stipulate a mark to be included in commercial electronic email which contains sexually oriented content.[88] The new FTC rule dictates that spam which contains sexually oriented material must now include the warning "SEXUALLY-EXPLICIT:" within the subject line, otherwise

---

[82] *Id.* at 309-10; *see also* Sabra-Anne Klein, *State Regulation of Unsolicited Commercial E-mail*, 16 BERKELEY TECH. L.J. 435, 444-45 (2001).

[83] Blanke, *supra* note 79, at 311.

[84] *Id.*

[85] "This Act supersedes any statute, regulation, or rule of a State or political subdivision of a State that expressly regulates the use of electronic mail to send commercial messages, except to the extent that any such statute, regulation, or rule prohibits falsity or deception in any portion of a commercial electronic mail message..." 15 U.S.C. § 7707(b)(1).

[86] Blanke, *supra* note 79, at 317. Marks, *supra* note 69, at 955-56.

[87] Blanke, *supra* note 79, at 311-12. Alepin, *supra* note 77, at 56.

[88] 15 U.S.C. § 7704(d).

the spammer may face a fine.[89] Sexually oriented material covers both written descriptions and visual images of sexually explicit conduct.[90]

Other provisions of CAN-SPAM mandated action by the FTC this year. Section 7708 required the FTC to submit to the Commerce Committee a plan and timetable for establishing a Do-Not-E-Mail registry within the first 6 months of 2004.[91] In June, the FTC informed Congress that such a registry could not be enforced effectively and would likely fail to reduce the amount of spam consumers receive, and in fact potentially increasing it.[92] The FTC noted the importance of the development of an effective means of email authentication as a precursor to implementing the registry.[93] Section 7702 of the act called for the FTC to promulgate regulations defining the criteria for determining the primary purpose of an email.[94] The FTC issued the regulations, effective March 28, 2005.[95]

B. STATE LEGISLATION

Five states enacted legislation directed at UCE in 2004: California, Florida, Maryland, Michigan, and Utah.[96] California Senate Bill 1457 was enacted on September 17, 2004, amending Section 17529.5 of the California Business and Professions Code so as to conform to the

---

[89] Label for E-Mail Messages Containing Sexually Oriented Material; Final Rule, 69 Fed. Reg. 21,023, 21,028 (April 19, 2004) (to be codified at 16 C.F.R. pt. 316), *available at* http://www.ftc.gov/os/2004/04/040413adultemailfinalrule.pdf.

[90] *Id.* at 21,032.

[91] 15 U.S.C. at § 7708(a).

[92] FEDERAL TRADE COMMISSION, NATIONAL DO NOT EMAIL REGISTRY, A REPORT TO CONGRESS, (June 2004), *available at* http://www.ftc.gov/reports/dneregistry/report.pdf.

[93] *Id.* at 37. *See infra* note 96.

[94] 15 U.S.C. at § 7702(2)(C).

[95] FEDERAL TRADE COMMISSION, DEFINITIONS AND IMPLEMENTATION UNDER THE CAN-SPAM ACT (August 13, 2004), *available at* http://www.ftc.gov/os/2005/01/050112canspamfrn.pdf.

[96] The House bill in Utah and Michigan both addressed child protection issues and will be discussed in a subsequent section. *Infra*, Part VIII. Additionally, bills were introduced in 25 states. Worth noting, Ohio H.B. 383 regarding UCE, was signed by the governor on February 1, 2005. *See* NATIONAL CONFERENCE OF STATE LEGISLATURES, UNSOLICITED COMMERCIAL E-MAIL ADVERTISEMENTS (ANTI-SPAM LEGISLATION) 2004 LEGISLATIVE ACTIVITY (April 2, 2005), *available at* http://www.ncsl.org/programs/lis/legislation/spam04.htm.

requirements set forth in CAN-SPAM.[97] Commercial email is defined so as to include both solicited and unsolicited advertisements.[98] Individuals or entities are prohibited from sending, either from or to a California email address, email containing false, misrepresented or misleading information, or including deceptive statements.[99] The bill authorizes the recipient of the offending email, the email service provider, and/or the Attorney General to commence action.[100]

In May of 2004, Florida enacted the Electronic Mail Communications Act, directed at deceptive and unsolicited commercial electronic email.[101] The Florida law differs from California in that it is directed solely at unsolicited commercial email, though it has a similar jurisdictional provision. The law prohibits using false or misrepresentative information regarding the routing or point of origin of an UCE, as well as prohibiting false or deceptive content in the subject line or message body.[102] The bill empowers recipients of violating email to bring a cause of action, as well as authorizes enforcement by the Florida Department of Legal Affairs.[103]

Also, in May, Maryland enacted the Maryland Spam Deterrence Act, encompassing many of the same features as the aforementioned state laws.[104] At present, the applicability of the law is unclear, as a Maryland circuit court judge has declared the law to be unconstitutional.[105]

The state of Utah has repealed the statute that had been enacted to address spam. Additionally, the Utah Senate repealed the Unsolicited

---

[97] CAL. BUS. & PROF. CODE § 17529.5 (West 2004).

[98] § 17529.5(a).

[99] § 17529.5(a)(1), (2).

[100] § 17529.5(b).

[101] S. B. 2574, 2004 Leg., Reg. Sess. (Fla. 2004) (codified at Fla. Stat. ch. 668.60- .6075 (2004)).

[102] FLA. STAT. ch. 668.603 (2004).

[103] ch. 668.606.

[104] S. B. 604, 2004 Leg., Reg. Sess. (Md. 2004) (codified at MD. CODE ANN., CRIM. LAW § 3-805 (2004)).

[105] *See infra* note 136.

Commercial and Sexually Explicit Email Act, probably as a response to the preemption provision of CAN-SPAM.[106]

C. FEDERAL LITIGATION

2004 marked the first opportunity for the FTC to enforce CAN-SPAM.[107] In April, the FTC filed a complaint against Phoenix Avatar, based out of Detroit, and Global Web Promotions, based out of Australia and New Zealand.[108] In addition, the U.S. Attorney's Office filed a criminal complaint which included allegations of criminal violations of CAN-SPAM.[109]

In *Phoenix Avatar*, the FTC alleged violations of the FTC Act and CAN-SPAM for the defendants' use of spam to sell diet patches.[110] With regard to CAN-SPAM, the FTC alleged that the defendants initiated the transmission of commercial email containing materially false or misleading heading information in violation of 15 U.S.C. § 7704(a)(1).[111] Additionally, defendants' commercial email allegedly did not provide clear and conspicuous notice to decline receipt, nor a valid physical postal address of the sender, both violations of § 7704(a)(5).[112] The case is pending, although a Temporary Restraining Order has been entered and a Preliminary Injunction issued, freezing

---

[106] S.B. 92, 2004 Gen. Sess. (Utah 2004) (repealing UTAH CODE ANN. § 13-36-101-105).

[107] In addition, the FTC settled two claims against spammers brought prior to the enactment of CAN-SPAM. *See* Stipulated Final Judgment, Federal Trade Commission v. Westby, No. 03-C-2540 (N.D. Ill. filed May 6, 2004) *available at* http://www.ftc.gov/os/caselist/0323030/040506ord0323030.pdf; stipulated Final Order, F.T.C. v. D Squared Solutions, Civ. No. AMD03CV3108 (D. Md. filed Aug. 9, 2005) *available at* http://www.ftc.gov/os/caselist/0323223/040809order0323223.pdf.

[108] F.T.C. v. Phoenix Avatar, No. 044C-2897 (N.D. Ill. filed April 29, 2004); *see generally* http://www.ftc.gov/os/caselist/0423084/0423084.htm; F.T.C. v. Global Web Promotions, No. 04C-3022 (N.D. Ill. filed April 29, 2004); *see generally* http://www.ftc.gov/os/caselist/0423086/0423086.htm.

[109] U.S. v. Lin, No. 04-80383 (E.D. Mich. filed April 29, 2004).

[110] Complaint for Injunctive and Other Equitable Relief at 9-11, Phoenix Avatar, No. 044C-2897, *available at* http://www.ftc.gov/os/caselist/0423084/040429phoenixavatarcomplaint.pdf (the Section 5 claims alleged that the diet patches did not function as claimed in the spam).

[111] *Id.* at 11.

[112] *Id.*

defendants' assets and enjoining defendants from engaging in illegal spamming and making deceptive product claims.[113]

In *Global Web Promotions*, the FTC alleges similar violations of both the FTC Act and CAN-SPAM for defendants' sale of diet patches and human growth hormone products via commercial email.[114] The FTC alleges the same specific violations of CAN-SPAM as in *Phoenix Avatar*. The FTC has filed for a Temporary Restraining Order, and the case is pending.[115]

In July of 2004, the FTC filed a complaint against Creaghan Harry, a Florida man, for allegedly using spam to sell counterfeit human growth hormone products.[116] The complaint invokes both the FTC Act and CAN-SPAM, alleging similar violations as in the complaints filed in April: disguising the emails' source, failing to provide clear and conspicuous notice of a consumer opt-out, and failing to provide a physical postal address.[117] The judge has issued a temporary restraining order, and the case is pending.[118]

The year 2004 saw the first criminal conviction under CAN-SPAM. In September, Nicholas Tombros pled guilty to one count of unauthorized access to a computer to send multiple commercial email messages.[119] Tombros engaged in "war-spamming," or searching for

---

[113] Stipulation and Order, Phoenix Avatar, No. 044C-2897, *available at* http://www.ftc.gov/os/caselist/0423084/040506tro0423084.pdf (last visited Feb. 19, 2005); Preliminary Injunction, Phoenix Avatar (No. 044C-2897), *available at* http://www.ftc.gov/os/caselist/0423084/040506pi0423084.pdf (last visited Feb. 19, 2005).

[114] Complaint for Injunctive and Other Equitable Relief at 9-14, Global Web Promotions, No. 04C-3022, *available at* http://www.ftc.gov/os/caselist/0423086/040428globalwebcomplaint.pdf (last visited Feb. 19, 2005).

[115] Memorandum Supporting Plaintiff's Motion for Temporary Restraining Order, Global Web Promotions, No. 04C-3022, *available at* http://www.ftc.gov/os/caselist/0423086/040428globalwebmemosupporting.pdf (last visited Mar. 12, 2005).

[116] F.T.C. v. Harry, No. 04C-4790 (N.D. Ill. filed July 21, 2004); *see generally* http://www.ftc.gov/os/caselist/0423085/0423085.htm.

[117] Complaint for Injunctive and Other Equitable Relief, Harry (No. 04C-4790), *available at* http://www.ftc.gov/os/caselist/0423085/040729cmp0423085.pdf (last visited Feb. 19, 2005).

[118] Temporary Restraining Order, Harry, No. 04C-4790, *available at* http://www.ftc.gov/os/caselist/0423085/040729tro0423085.pdf (last visited Feb. 19, 2005). In a similar action, the FTC has enjoined a Florida business from sending spam promoting an allegedly bogus money-making scheme. *See* F.T.C. v. Bryant, No. 3:04-CV-897-J-32MMH, 2004 WL 2504357 (M.D. Fla. Oct. 4, 2004).

[119] Press Release, Debra W. Yang, U.S. Att'y C.D. Cal., Guilty Plea by Local 'War-Spammer' is First-Ever Conviction Under CAN-SPAM Act (Sept. 28, 2004), *available at*

unprotected wireless access points and then using these access points to send spam.[120]

In addition to criminal and civil enforcement by the government, several private companies brought civil actions as empowered under section 7706(g) of CAN-SPAM. The first suit was brought by Hypertouch, Inc., a small ISP.[121] Hypertouch alleges violation of section 7705 of the Act, accusing defendant domain name owner of sending commercial email with false header information to individuals who specified that they did not want to receive them.[122]

Civil actions were also brought by larger ISPs. Microsoft, AOL, Earthlink, and Yahoo! coordinated the filing of six lawsuits on March 9, 2004.[123] The complaints make similar accusations, alleging that defendants initiated the transmission of emails containing header information which is materially false or materially misleading in violation of section 7704(a)(1), contained subject headings likely to mislead the recipient in violation of section 7704(2), failed to provide a functioning return email address in violation of section 7704(3), and failed to include clear and conspicuous identification of solicitation, opt-out or a valid postal address in violation of section 7704(5).[124] The plaintiffs are seeking injunctive relief as well as damages.

---

http://www.usdoj.gov/usao/cac/pr2004/131.html. *See* U.S. v. Tombros, No. CR-04-1085 (C.D. Cal. Sept. 27, 2004).

[120] Press Release, Yang, *supra* note 119.

[121] Hypertouch, Inc. v. BVWebTies, No. 3:04-CV-00880-MMC (N.D. Cal. 2004) (filed Mar. 4, 2004).

[122] Complaint, Hypertouch v. BVWebTies, No. 3:04-CV-00880-MMC (N.D. Cal. filed Mar. 4, 2004), *available at* http://legal.hypertouch.com/bobvila/bobvila-complaint.html.

[123] Complaint, America Online v. John Does 1-40, No. 04-260-A (E.D. Va. March 9, 2004) *available at* http://www.gigalaw.com/canspam/aol-does-complaint-2004-03-09.pdf; Complaint, AOL v. Hawke, No. 04-259-A (E.D. Va. filed March 9, 2004) *available at* http://www.gigalaw.com/canspam/aol-hawke-complaint-2004-03-09.pdf; Complaint, Earthlink v. John Does 1-25, No. 04CV-0667 (N.D. Ga. filed March 9, 2004) *available at* http://www.earthlink.net/about/press/pr_AllianceFAS/EarthLink_CAN_SPAM_Filed_Stamped.pdf; Complaint, Microsoft v. JDO Media, No. CV04-0517 (W.D. Wa. filed March 9, 2004) *available at* http://www.gigalaw.com/canspam/microsoft-jdo-complaint-2004-03-09.pdf; Complaint, Microsoft v. John Does 1-50, No. CV04-0516 (W.D. Wa. filed March 9, 2004) *available at* http://www.gigalaw.com/canspam/microsoft-does-complaint-2004-03-09.pdf; Complaint, Yahoo v. Head, No. C04-00965 (N.D. Cal. filed March 9, 2004) *available at* http://docs.yahoo.com/docs/pr/pdf/complaint.pdf.

[124] *Id.* Additional arguments are set forth under different legal basis, including trespass to chattels, conversion, violation of the Computer Fraud and Abuse Act, and the Lanham Act.

Other cases have raised interesting issues relating to spam. In Iowa, a federal judge entered a default judgment in excess of $1 billion dollars against spammers sending UCE to an Iowa ISP.[125] In a Florida bankruptcy court, an individual subject to a $6.9 million judgment for ignoring a court order to cease sending UCE to AOL has been denied the use of Chapter 7 bankruptcy as a means to avoid the judgment.[126] In Texas, a court held that while CAN-SPAM preempts particular anti-spam statutes, it expressly allows computer system owners to block incoming spam.[127] At issue in the case is whether the University of Texas acted unlawfully in blocking UCE from an online dating service directed towards the University's computer system. This case is likely to generate the first appellate ruling regarding CAN-SPAM.

D. STATE LITIGATION

At the state level, civil actions were filed by both government and private parties. The state of Massachusetts was the first state to file under CAN-SPAM. The Massachusetts Attorney General brought an action against a Florida business for failure to identify UCE as advertisements, failure to include an opt-out provision, and the use of a non-functioning sender address.[128] The state also alleges violations of the Massachusetts Consumer Protection Act.[129]

In 2003, New York Attorney General Elliot Spitzer brought actions against several companies allegedly transmitting UCE in violation of New York consumer protection law.[130] Spitzer alleged use of fake names, spoofing of well-known corporate names, deceptive subject

---

[125] Kramer v. Cash Link Systems, No. 3-03-CV-80109-CRW-TJ, 2004 WL 2952561, at *5-7 (S.D. Iowa filed Dec. 17, 2004) (adjudicating Iowa law, not CAN-SPAM).

[126] America Online v. Uhrig, Bankr. No. 01-21251-8B1, 2004 WL 414996 (Bankr. M.D. Fla. Feb. 26, 2004).

[127] White Buffalo Ventures v. Univ. of Texas, No. A-03-CA-296-SS, 2004 WL 1854168 (W.D. Tex. Mar. 22, 2004).

[128] Complaint, Massachusetts v. DC Enterprises, (Mass. Super. Ct. filed July 1, 2004) *available at* http://www.gigalaw.com/canspam/massachusetts-dcenterprises-2004-07-01.pdf.

[129] MASS. GEN. LAWS ch. 93A (2005).

[130] People v. Synergy6, No. 404027/2003 (N.Y. Sup. Ct. filed May 28, 2004).

lines, and endeavoring to conceal the emails' true source.[131] In July 2004, Spitzer settled with one of the litigants, OptInRealBig.com.

Microsoft was a prominent litigant at the state level. In addition to assisting Spitzer with the lawsuit brought in New York, Microsoft filed a number of private actions. In the beginning of June, Microsoft filed eight separate lawsuits against John Does and named parties, alleging a variety of violations of the Washington Commercial Electronic Mail Act, the Washington Consumer Protection Act, the CAN-SPAM Act, and the Lanham Act.[132] Microsoft also brought an action against a hosting company which provides "bulletproof" services, meaning the company refuses to terminate a customer for spamming.[133] Microsoft raises claims similar to the aforementioned lawsuits, but also specifically addresses the practices of bulletproof spammers. Microsoft claims such companies target their services specifically to spammers and maintain offshore servers so as to avoid the reach of law enforcement within the U.S.[134]

Two cases show contradictory trends in state anti-spam statutes. In an action brought under Washington's anti-spam law, the state court of appeals affirmed a civil fine and award of attorney fees rendered against an Oregon resident for transmitting deceptive and misleading

---

[131] Press Release, Eliot Spitzer, New York State Attorney General, Spitzer Announces Settlement, Set Strict Standards, for Deceptive Spammer (July 19, 2004) *available at* http://www.oag.state.ny.us/press/2004/jul/jul19a_04.html.

[132] Complaint, Microsoft v. John Does 1-50, No. 04-2-13120-1 (Super. Ct. Wash. filed June 9, 2004) *available at* http://www.gigalaw.com/canspam/microsoft-does-1-50-complaint-2004-06-09.pdf; Complaint, Microsoft v. John Does 1-20, No. 04-2-13324-6 (Super. Ct. Wash. filed June 9, 2004) *available at* http://www.gigalaw.com/canspam/microsoft-does-1-20-complaint-2004-06-09.pdf; Complaint, Microsoft v. John Does 1-20, No. 04-2-13130-8 (Super. Ct. Wash. filed June 9, 2004) *available at* http://www.gigalaw.com/canspam/microsoft-does-1-20(2)-complaint-2004-06-09.pdf; Microsoft v. John Does 1-20, No. 04-2-13119-7 (Super. Ct. Wash. filed June 9, 2004) available at http://www.gigalaw.com/canspam/microsoft-does-1-20(3)-complaint-2004-06-09.pdf; Microsoft v. Hites, No. 04-2-12434-4 (Super. Ct. Wash. filed June 2, 2004) *available at* http://www.gigalaw.com/canspam/microsoft-hites-complaint-2004-06-02.pdf; Microsoft v. Pin Point Media, No. 04-2-12467-1 (Super. Ct. Wash. filed June 2, 2005) *available at* http://www.gigalaw.com/canspam/microsoft-pinpoint-complaint-2004-06-02.pdf; Microsoft v. John Does 1-50, No. 04-2-12465-4 (Super. Ct. Wash. filed June 2, 2004) *available at* http://www.gigalaw.com/canspam/microsoft-does-1-50-complaint-2004-06-02.pdf; Microsoft v. John Does 1-20, No. 04-2-12433-6 (Super. Ct. Wash. filed June 2, 2004) *available at* http://www.gigalaw.com/canspam/microsoft-does-1-20-complaint-2004-06-02.pdf.

[133] Complaint, Microsoft v. Gillespie, No. 04-2-23937-1, 2004 WL 2157242 (Super. Ct. Wash. filed Sept. 13, 2004).

[134] *Id.*

commercial spam to Washington residents.[135] On the other end of the spectrum, a circuit court judge in Maryland has declared Maryland's Commercial Electronic Email Act unconstitutional for violation of the dormant Commerce Clause.[136] Although the Maryland statute is structured so as to avoid preemption under CAN-SPAM, the judge found that in this instance, the Maryland statute sought to regulate conduct between people outside the state of Maryland.[137]

E. CONCLUSION

In spite of CAN-SPAM and enforcement at the federal and state level, spam is a continuing problem. The FTC has noted that while email is of great benefit to both consumers and businesses, "the increasing volume of spam to ISPs, to businesses, and to consumers, coupled with the use of spam as a means to perpetuate fraud and deception put these benefits [of email] at serious risk."[138] As spam is a continuing problem, solutions will continue to be sought legislatively, administratively, and in the private sector.[139]

IV. PHISHING AND SPOOFING

Intertwined with the issue of spam is phishing (or web page spoofing), the fraudulent acquisition of sensitive personal information by use of deception.[140] Typically, an Internet scammer will utilize spam email or pop-up messages to deceive an individual into believing he or she is dealing with someone trustworthy. The individual will then be directed to a web page that has the look and feel of the trusted

---

[135] State v. Heckel, 93 P.3d 189 (Wash. Ct. App. 2004).

[136] MaryCLE v. First Choice Internet, No. 248514, 2004 WL 2895955 (Md. Cir. Ct. Dec. 9, 2004).

[137] *Id.* at *4.

[138] Federal Trade Commission, Prepared Statement of the Federal Trade Commission on "Unsolicited Commercial Email" Before the Senate Committee on Commerce, Science and Transportation 16 (May 21, 2003), *available at* http://www.ftc.gov/os/2003/05/spamtestimony.pdf.

[139] One specific example is the FTC's belief that email authentication may act as a predicate for reducing spam. *See* Email Authentication Summit Notice, 69 Fed. Reg. 55633 (Sept. 15, 2004), *available at* http://www.ftc.gov/os/2004/09/040915emailauthfrn.pdf.

[140] *Phishing*, Wikipedia, *at* http://en.wikipedia.org/wiki/Phishing (last visited Feb. 15, 2005).

page, but is in fact owned and operated by someone else. Having fooled the consumer into believing he or she is accessing a trusted site, the scammer will then ask that individual for sensitive information such as credit card numbers, bank account information, Social Security numbers, or passwords.[141]

A phishing attack may take a number of increasingly sophisticated forms. Often the scammer will use URL spoofing to deceive the consumer into believing he or she is accessing a trusted website. This may involve using a similar sounding, yet fake, domain name or substituting a letter from an existing legitimate domain name.[142] Often after receiving the desired information, the scammer will redirect the consumer to the legitimate website which the scammer has spoofed. This gives the transaction an air of legitimacy, lessening the likelihood that a consumer would realize that a fraud has been perpetrated and that there is an incident to report. The degree of sophistication invoked in phishing attacks, however, has escalated beyond these traditional tactics.

An emerging trend in phishing attacks is the use of malcode. The Internet scammer will send the consumer to a URL spoof which hosts a malicious software application or contains covertly downloaded and malicious scripts.[143] Once this application is downloaded on the consumer's computer, there are two variations on the subsequent attack. First, the malicious scripts may modify the host file[144] located on the consumer's computer, such that when the consumer enters the web address for a legitimate website, the address actually takes the consumer to a spoofed site where he or she is vulnerable to identity

---

[141] FEDERAL TRADE COMMISSION, HOW NOT TO GET HOOKED BY A 'PHISHING' SCAM (June 2004) *available at* http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm.

[142] E-mail Spam, *supra* note 65.

[143] ANTI-PHISHING WORKING GROUP, PHISHING ACTIVITY TRENDS REPORT (Dec. 2004), *at* http://www.antiphishing.org/APWG%20Phishing%20Activity%20Report%20-%20December%202004.pdf.

[144] "In computing, a **host file**, stored on the computer's filesystem, is used to look up the Internet Protocol address of a device connected to a computer network. The host file describes a many-to-one mapping of device names to IP addresses. When accessing a device by name, the networking system will attempt to locate the name within the host file if it exists. Typically, this is used as a first means of locating the address of a system, before accessing the Internet domain name system. The reason for this is that the host file is stored on the computer itself and does not require any network access to be used, whereas DNS requires access to an external system, which is typically slower." *Host File*, Wikipedia, http://en.wikipedia.org/wiki/Host_file (last visited May 7, 2005).

theft. Second, malicious software may install key-loggers, allowing information to be sent from the consumer's computer to the attacker when specific, predetermined sites are accessed.[145]

Phishing raises serious concerns for both businesses and individual consumers. A recent survey conducted by Gartner, Inc., an ICT research and analysis firm, estimated the direct losses suffered by banks and credit card issuers from phishing attacks to be approximately $1.2 billion dollars in 2003.[146] Another survey conducted by CSO magazine in conjunction with the CERT Coordination Center and the U.S. Secret Service, found that other harmful impacts from phishing may include disruption within the organization, harm caused to the organization's reputation, customer loss, or critical system disruption.[147] With regard to individual consumers, a study by the Ponemon Institute, sponsored by TRUSTe, estimated that victims' monetary loss due to phishing attacks was approximately $500 million.[148]

Phishing's relation to identity theft causes it to fall under the strictures of a myriad of regulation. At the federal level, an Internet scammer may be committing identity theft,[149] wire fraud,[150] credit card fraud,[151] bank fraud,[152] computer fraud,[153] and violations considered

---

[145] *Id.*

[146] Press Release, Gartner, Gartner Study Finds Significant Increase in E-Mail Phishing Attacks (May 6, 2004), *at* http://www4.gartner.com/press_releases/asset_71087_11.html.

[147] CARNEGIE-MELLON SOFTWARE ENGINEERING INSITTUTE, 2004 E-Crime Watch Survey Summary of Findings 13 (2004), *available at* http://www.cert.org/archive/pdf/2004eCrimeWatchSummary.pdf.

[148] TRUSTE, U.S. Consumer Loss of Phishing Fraud to Reach $500 Million, (Sept. 29, 2004), *at* http://www.truste.org/cgi-dada/mail.cgi?flavor=archive&id=20040929191710&list=Press_Releases.

[149] 18 U.S.C. § 1028(a)(7); 18 U.S.C. § 1028A (2005).

[150] 18 U.S.C. § 1343.

[151] 18 U.S.C. § 1029.

[152] 18 U.S.C. § 1344.

[153] 18 U.S.C. § 1030(a)(4).

criminal offenses under the CAN-SPAM Act.[154] If the phishing attack utilizes a computer virus or worm, the scammer may be violating provisions of the computer fraud and abuse statute that relate to damaging computer systems and files.[155] Additionally, the Federal Trade Commission may invoke its consumer protection power under Section 5 of the Federal Trade Commission Act, which states that "unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are declared... unlawful."[156] Under Section 5, the FTC may seek civil penalties or consumer redress. Further, if the personal information involves financial information, the FTC may bring enforcement action under the Gramm-Leach-Bliley Act.[157] At the state level, action could be brought by the state attorney general for fraud or identity theft.

A. FEDERAL LEGISLATION

In July of 2004, President Bush signed the Identity Theft Penalty Enhancement Act ("ITPEA"), establishing the federal criminal offense of aggravated identity theft.[158] An individual commits aggravated identity theft if, while engaging in an enumerated identity theft related offense, the individual "knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person."[159] The commission of aggravated identity theft results in a mandatory minimum sentence of 2 years imprisonment in addition to the punishment imposed for the enumerated felony.[160] This law indirectly impacts the practice of phishing by creating a more stringent means to punish Internet scammers engaging in phishing attacks.

Legislation directly aimed at the practice of phishing was introduced by Democratic Senator Patrick Leahy of Vermont in the

---

[154] 18 U.S.C. § 1037. *See also* DEPARTMENT OF JUSTICE, CRIMINAL DIVISION, SPECIAL REPORT ON "PHISHING", *available at* http://www.usdoj.gov/criminal/fraud/Phishing.pdf (last visited Feb. 16, 2005).

[155] 18 U.S.C. § 1028(a)(5).

[156] 15 U.S.C. § 45(a)(1).

[157] 15 U.S.C. § 6801-6809.

[158] 18 U.S.C. § 1028A (2005).

[159] 18 U.S.C. § 1028A(a)(1).

[160] *Id.*

108th Congress. The Anti-Phishing Act of 2004[161] is intended to "criminalize Internet scams involving fraudulently obtaining personal information, commonly known as phishing."[162] The congressional findings section of the bill notes society's increased dependence on the Internet for communication, consumer and financial transactions, and the critical importance of establishing the Internet as a trustworthy medium in order for it to reach its full potential.[163]

The statute seeks to amend the fraud and identity statute with the addition of Internet fraud.[164] The statute is directed at those "with the intent to carry on any activity which would be a Federal or State crime of fraud or identity theft."[165] If such an individual knowingly engages in cybersquatting[166] or spoofs a domain name to induce or solicit an individual to provide information, he may be subject to a fine, imprisonment, or both.[167] Additionally, if such an individual sends an email or other Internet communication, which falsely represents itself as being sent by a legitimate business, refers or links users to a cybersquatted or spoofed location, and induces or solicits personal information, he may be subject to the same punishment.[168]

The most notable feature of the Anti-Phishing Act is that it criminalizes conduct engaged in before the actual commission of the fraud. At present, the law is equipped to handle instances in which actual fraud has occurred. The Anti-Phishing Act seeks to pre-empt the commission of a fraud by criminalizing behavior whose only purpose would lead to perpetration of a fraud. The Bill has been sent to the Senate Judiciary Committee.

---

[161] S. 2636, 108th Cong. (2004).

[162] *Id.* at title.

[163] *Id.* at § 2.

[164] *Id.* at § 3-1351.

[165] *Id.*

[166] *See Cybersquatting*, WIKIPEDIA, *at* http://en.wikipedia.org/wiki/Cybersquatting (last visited Feb. 17, 2005).

[167] S. 2636, 108th Cong. § 3 (2004).

[168] *Id.* at § 3-1351(b)(3).

B. LITIGATION

The most prominent legal action regarding phishing in the past year was a joint initiative between the Federal Trade Commission and the Department of Justice. Zachary Hill operated a spam operation which used logos from America Online ("AOL") and Paypal to deceive consumers into providing credit card and bank account numbers.[169] The scam functioned as follows: Consumers received an email that appeared as though it was sent from AOL or Paypal. The "from" line identified the sender of the email as "billing center" or something similar, and the "subject" line typically contained a warning regarding a billing error or a need to update account information.[170] The body of the email would threaten the consumer with cancellation of his account if no response was made. An embedded hyperlink would then take the consumer to a page which appeared to be the AOL or Paypal billing center where the consumer was then asked to provide personal information.[171] This personal information was subsequently used to access consumers' Paypal accounts for the purpose of purchasing goods or services, as well as to use consumers' credit card information to place orders and make purchases.[172]

The FTC brought a civil action alleging that Hill engaged in deceptive and unfair acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a) and Section 521 of the Gramm-Leach-Bliley Act, 15 U.S.C. § 6821.[173] The matter was resolved via a Stipulated Final Judgment.[174] The settlement prohibits Hill from sending unsolicited commercial email, and bars him from: misrepresenting his affiliation with a consumer's ISP, misrepresenting to consumers that their information needs updating, using false "from"

---

[169] Press Release, FTC, FTC, Justice Department Halt Identity Theft Scam (March 22, 2004), *available at* http://www.ftc.gov/opa/2004/03/phishinghilljoint.htm.

[170] *Id.*

[171] *Id.*

[172] *Id.*

[173] Complaint for Permanent Injunction and Other Equitable Relief (S.D. Tex.filed Dec. 3, 2003), Federal Trade Commission v. Hill, No. H-03-5537, *available at* http://www.ftc.gov/os/caselist/0323102/040322cmp0323102.pdf.

[174] Stipulated Final Judgment and Order for Permanent Injunction and Other Equitable Relief, Federal Trade Commission v. Hill, No. H-03-5537 (S.D. Tex. filed May 18, 2004), *available at* http://www.ftc.gov/os/2004/06/040518stiphill.pdf.

or "subject" lines, and registering Web pages that misrepresent the host of the page.[175] Judgment was further entered against Hill in the amount of $125,000 for consumer redress; however, the judgment was stayed and considered satisfied contingent on the truthfulness and accuracy of a financial statement provided by Hill.[176]

In addition to the settlement with the FTC, Hill was subject to prosecution by the Department of Justice. The DOJ brought a two count criminal indictment: Count I alleged possession of credit card numbers, bank account numbers, and other access devices with the intent to defraud in violation of 18 U.S.C. § 1029(a)(3), and Count II alleged use of said devices to defraud others in violation of 18 U.S.C. § 1029(a)(5).[177] Hill entered into a plea agreement, which resulted in his being sentenced to 46 months in prison.

Also stemming from the AOL and Paypal phishing attacks, the FTC brought an action against then-minor Michael Maloney. The FTC alleged the same violations which were engaged in by Hill. Maloney entered into a Stipulated Final Judgment with similar terms to that of Hill.[178]

C. CONCLUSION

Phishing attacks show no sign of slowing down or stopping. The Anti-Phishing Working Group notes that the average monthly growth rate for new unique phishing email messages from July through December 2004 was 38%.[179] Over the same time period, the number of phishing websites supporting the attacks grew at a 24% rate.[180] Legislation and litigation appears more focused on the broader issue of spam, however. It is possible that the *Hill* case represents an emerging federal focus on phishing attacks. Phishing certainly presents an

---

[175] F.T.C., "PHISHERS" SETTLE FEDERAL TRADE COMMISSION CHARGES (June 17, 2004), *available at* http://www.ftc.gov/opa/2004/06/hill.htm.

[176] *Hill*, Stipulated Final Judgment at 10.

[177] Criminal Information, *United States v. Hill* (E.D. Va.), *available at* http://www.ftc.gov/os/caselist/0323102/040322info0323102.pdf (last visited Feb. 17, 2005).

[178] Stipulated Final Judgment and Order for Permanent Injunction and Other Equitable Relief, Federal Trade Commission v. _____, a minor (E.D. N.Y. filed May 18, 2004), *available at* http://www.ftc.gov/os/2004/06/040518stipaminorbyhisparents.pdf.

[179] ANTI-PHISHING WORKING GROUP, *supra* note 143, at 2.

[180] *Id.*

economic concern both to businesses and consumers. The continued growth of phishing attacks and sites supporting attacks indicate that phishing is unlikely to subside in the near future.

V. INTERNET GOVERNANCE: WHOIS DATABASES

A major development in 2004 concerning privacy and the WHOIS databases was the passage of the Fraudulent Online Identity Sanctions Act ("FOISA").[181] Before discussing FOISA and other WHOIS activity in 2004, a brief background on WHOIS is necessary. The WHOIS (pronounced as two separate words: "who is") databases are a series of publicly accessible databases that maintain contact information for domain name owners, such as name, address, email address, and telephone information.[182] Technically, WHOIS is not the database, itself, but "a protocol for submitting a query to a database" in order to find contact information for the owner of a domain name.[183] For the purposes of this paper, the term "WHOIS" will be used to refer to the database systems themselves.

The Internet Corporation for Assigned Names and Numbers ("ICANN") is responsible for setting guidelines for various aspects of the Internet, including WHOIS.[184] ICANN states that its policy reason for having "[i]nformation about *who is* responsible for domain names ... publicly available" is "to allow rapid resolution of technical problems and to permit enforcement of consumer protection, trademark, and other laws."[185] From a practical point of view, however, this statement means that every person who wants to register a domain name either consents to put some sort of publicly accessible contact information on line, or is unable to register the domain name. This has led to a number of creative solutions for those who do not

---

[181] *See* Intellectual Property Protection and Courts Amendments Act of 2004, Pub. L. No. 108-482, §§ 201-05 (2004).

[182] An example of a domain name is <amazon.com> or <google.com>.

[183] *Whois*, WIKIPEDIA, *at* http://en.wikipedia.org/wiki/Whois (last visited Mar. 13, 2005).

[184] *See* ICANN, FAQs, *at* http://icann.org/faq/#whois (last modified Jun. 9, 2004). *See also* Verisign v. ICANN, 2004 WL 2095696, at *2-3 (C.D. Cal. 2004) (granting ICANN's motion to dismiss "claim one of the F[irst] A[lleged] C[omplaint]" because VeriSign did not plead enough facts to "establish that ICANN's Board was a 'rubber stamp'" and mentioning "ICANN's rather formidable challenge[] ... to promote coherent policies ... in the business of 'cyberspace.'").

[185] ICANN, FAQs, *supra* note 184 (emphasis added).

want their personal contact information published on the Internet, from people providing "inaccurate WHOIS information" to companies that will register domain names for individuals and act as a proxy by using the company's contact information. Both methods are efforts by people "to protect their privacy and protect their personally identifiable information from being globally, publicly accessible."[186]

ICANN is aware of the WHOIS privacy issue and "established three Task Forces to develop policy for the WHOIS database."[187] In May of 2004, the three task forces issued preliminary reports, sought comments on the reports, and issued some broad recommendations.[188] Among the issues considered by the task forces was bulk access, where the publicly accessible information can be queried in an automated manner.[189] A consensus was reached that bulk access to the WHOIS databases for "marketing purposes" was undesirable.[190] But "[i]t is not possible to create technical restrictions ... that will limit port 43 [bulk] access to a specific type of purpose[,] such as 'non-marketing uses[,]'" while still allowing access for other legitimate purposes.[191] One such legitimate purpose is propagating changes in

---

[186] *Whois: Privacy and Accuracy*, ELECTRONIC PRIVACY INFORMATION CENTER, *at* http://www.epic.org/privacy/whois/#privacyAccuracy (last visited Mar. 13, 2005); *see also Domain Name Proxy Agreement,* DOMAINS BY PROXY, INC. (defining the terms of the agreement, including when it will turn over the information to third parties), *at* http://domainsbyproxy.com/popup/DomainNameProxyAgreement.htm (last visited Mar. 13, 2005); *see also* Kim Zetter, *Domain Owners Lose Privacy* (Mar. 4, 2005) (the "U.S. Commerce Department has ordered companies that administer [I]nternet addresses to stop allowing customers to register .us domain names anonymously using proxy services" because it cannot verify that U.S. persons are the registrants of the domain name), *at* http://www.wired.com/news/privacy/0,1848,66787,00.html.

[187] *ICANN Taskforces Produce Preliminary Reports on WHOIS - Public Comment Period is NOW*, THE PUBLIC VOICE (June 2004), *at* http://www.thepublicvoice.org/news/2004_whoiscomments.html; *see also Whois Privacy*, ICANN, *at* http://gnso.icann.org/issues/whois-privacy/ (last visited Mar. 13, 2005).

[188] *See ICANN Releases 3 Whois Reports for Comments*, ICANN WATCH (May 30, 2004), *available at* http://www.icannwatch.org/article.pl?sid=04/05/30/2051217.

[189] *WHOIS Task Force 1 Restricting Access of WHOIS for Marketing Purposes Preliminary Report*, ICANN (May 2004), *at* http://gnso.icann.org/issues/whois-privacy/Whois-tf1-preliminary.html#DataMining.

[190] *Id.*

[191] *Id.*

WHOIS information between all of the companies that provide the service of domain name registration.[192]

ICANN is still considering the WHOIS privacy issues. In the meantime, Congress enacted the Fraudulent Online Identity Sanctions Act, which targets people who provide inaccurate contact information when registering a domain name.

A. FEDERAL LEGISLATION

The Fraudulent Online Identity Sanctions Act ("FOISA") took an interesting route through Congress. Originally introduced as H.R. 3754, the last official action occurred on June 9, 2004, when it was placed on the Union Calendar of the House of Representatives.[193] However, H.R. 3754 was eventually enacted as an amendment to H.R. 3632.

H.R. 3632 began as the Anti-Counterfeiting Amendments Act of 2004 and dealt with trafficking in counterfeit components.[194] The Congressional Record of September 21, 2004 records Representative Smith of Texas stating that "[t]he text of H.R. 3754, the Fraudulent Online Identity Sanctions Act, has also been included in the underlying legislation. The Fraudulent Online Identity Sanctions Act assures those that use false identities in conjunction with a domain name face additional penalties for other crimes they commit."[195] From there the bill, now known as the Intellectual Property Protection and Courts Amendments Act of 2004, went to the Senate and was approved without amendment, becoming Public Law 108-482.[196]

FOISA establishes the rebuttable presumption that people who provide inaccurate information to WHOIS and who then commit a

---

[192] *Id.*

[193] *Bill Summary & Status for the 108th Congress (for H.R. 3754, 108th Cong. (2004))*, LIBRARY OF CONGRESS, *available at* http://thomas.loc.gov/cgi-bin/bdquery/z?d108:HR03754:@@@X (last visited Mar. 13, 2005).

[194] *See Anti-Counterfeiting Amendments Act of 2004*, H.R. Rep. No. 108-600 (2004), *available at* http://thomas.loc.gov/cgi-bin/cpquery/R?cp108:FLD010:@1(hr600).

[195] 150 CONG. REC. H7264, H7267 (daily ed. September 21, 2004) (statement by Rep. Smith), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getpage.cgi?dbname=2004_record&page=H7267&position=all (last visited March 13, 2005).

[196] *Bill Summary & Status for the 108th Congress (for H.R. 3632, 108th Cong. (2004))*, LIBRARY OF CONGRESS, *available at* http://thomas.loc.gov/cgi-bin/bdquery/z?d108:HR03632:@@@X (last visited March 13, 2005)

crime, such as a trademark violation, copyright infringement, or felony, using the inaccurately registered domain name have willfully committed the crime, because they are obfuscating their contact information.[197] The law defines inaccurate information differently when committing a trademark violation or copyright infringement, requiring that the person "knowingly provided or knowingly caused to be provided materially false contact information to a domain name registrar, domain name registry, or other domain name registration authority in registering, maintaining, or renewing a domain name used in connection with the violation," than when committing a felony, which requires the defendant to have "knowingly falsely registered a domain name and knowingly used that domain name in the course of that offense."[198] The burden placed on the alleged intellectual property infringer or felon is large.

In regards to intellectual property, FOISA establishes a "rebuttable presumption" that the "violation is willful" or that the "infringement was committed willfully."[199] In copyright and trademark law, this is tantamount to a shift from injunctive relief, as actual damages are often difficult to prove, to seemingly punitive statutory damages, specifying that the "infringer sustains the burden of proving" that the infringement was not willful.[200]

For any felony conviction where the person knowingly used a falsely registered domain name while committing the felony, FOISA does not establish a rebuttable presumption but mandates an increased prison term.[201] For a person convicted of a felony that falls under FOISA, "the maximum imprisonment otherwise provided by law for that offense shall be doubled or increased by 7 years, whichever is less."[202] Further, for felonies, "falsely registered" is defined as to register "in a manner that prevents the effective identification of or

---

[197] Fraudulent Online Identity Sanctions Act, Pub. L. No. 108-482, §§ 202-04, 118 Stat. 3912 (2004).

[198] *Id.*

[199] *Id.* §§ 202-03.

[200] 17 U.S.C. § 504(c)(2) (2004); *see also* 15 U.S.C. § 1117(c)(2) (2004) (nonwillful statutory damages are capped per violation, with copyright at $30,000 trademark at $100,000; in the event that the conduct is willful, however, copyright statutory damages are capped at $150,000 and trademark at $1,000,000, with the defendant bearing the burden of proof).

[201] Pub. L. No. 108-482, § 204, 118 Stat. 3912 (2004).

[202] *Id.*

contact with the person who registers."[203] This seems to implicate more than just WHOIS. For example, registering a domain name with an active Yahoo! email address (a free email address) that itself has inaccurate information might prevent the "effective identification of or contact with the person who registers" because it obfuscates the actual identity of the domain name owner.[204]

FOISA provides that "[n]othing in this title shall enlarge or diminish any rights of free speech or of the press for activities related to the registration or use of domain names."[205] This provision appears to be an attempt to stymie the argument that people may register inaccurate information in WHOIS for purposes other than to commit crimes, such as anonymous free speech. But by establishing a rebuttable presumption of willfulness, people who do so will still have to go to court to prove that their conduct was protected speech. For example, if someone registers a domain name to protest certain work conditions anonymously and uses inaccurate information to register the domain name, that person's employer could bring a claim of trademark violation (e.g., for causing confusion about the company's mark) with a rebuttable presumption of willfulness against the person. Notwithstanding the language in FOISA, this rebuttable presumption may effectively discourage people from participating in free speech.

FOISA does not target Internet Protocol ("IP") addresses, which do not require registration and are primarily used in peer-to-peer file sharing, instant messaging, and other applications where the user does not necessarily know the destination computer that he is trying to access.

B. CONCLUSION

There are privacy concerns with the current WHOIS system. The fact that the contact information of every person who registers a domain name is publicly available has prompted some to register domain names with inaccurate information, in an attempt to shield privacy. ICANN has been looking into the problem for some time, and its three task forces are the latest attempt to define the problem and recommend a solution. On the other hand, some people use the Internet for illicit activities and use inaccurate information when

---

[203] *Id.*

[204] *See id.*

[205] *Id.* § 205.

registering domain names to hide their identity in order to evade law enforcement. FOISA attempts to target these people.

Unfortunately, there is no readily available solution to all of this. WHOIS, ICANN, and inaccurately registered domains are certainly going to remain an issue in 2005 and beyond. People will continue to advocate various solutions, from disabling WHOIS entirely or providing various levels of privacy protection in WHOIS, to leaving the system alone and mandating accurate information.

VI. FRAUD AND WRONGDOING

In 2004, fraud and wrongdoing regarding Internet privacy was addressed at both the federal and state level. Civil enforcement at the federal level falls under the auspices of the FTC. As briefly mentioned above, the FTC is charged with consumer protection, and under Section 5 of the FTC Act, may act to prevent "unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce."[206] The Commission is empowered to seek civil penalties or consumer redress via injunctive or other equitable relief.[207] The FTC may also endeavor in civil enforcement under CAN-SPAM and other statutory provisions.

Federal criminal enforcement is commonly brought under the Computer Fraud and Abuse Act ("CFAA").[208] Section 1030(a) lists seven prohibited actions. These are:

> 1) knowingly accessing a computer without authorization or in excess of one's authority and accessing classified government information;
>
> 2) intentionally accessing a computer without authorization and obtaining financial, government or other information;
>
> 3) accessing a government computer if access affects its use;
>
> 4) knowingly and with intent defraud, accessing a protected computer;

---

[206] 15 U.S.C. § 45(a)(1).

[207] § 45(m).

[208] 18 U.S.C. § 1030 (amended 1986, 1988, 1989, 1990, 1994, 1996, 2001, 2002).

5) computer vandalism;

6) knowingly and with intent to defraud, trafficking in password or similar information;

7) communicating a threat to damage a protected computer.[209]

An individual offending the provisions of these acts may be subject to a fine, imprisonment, or both.[210] In addition to the CFAA, other provisions of the United States Code bear on computer intrusion as well.[211]

At the state level, civil action is typically brought by the state attorney general. Most often the action is commenced based on allegations of deception or fraud and proceeds under the state attorney general's power to protect consumers. States are becoming more organized in addressing Internet privacy by creating specific offices to handle Internet related issues.[212]

In addition to consumer protection, some states have enacted laws specifically targeting Internet privacy policies. California has led the way in this regard, enacting legislation addressing both privacy policies and the required conduct following a breach of an individual's personal information.[213] California's Online Privacy Protection Act requires an operator of a website which collects personally identifiable information from California resident users to post the company's privacy policy conspicuously.[214] The privacy policy must (1) identify the categories of personally identifiable information collected and the categories of persons or entities with whom the operator shares such

---

[209] § 1030(a)(1-7).

[210] § 1030(c).

[211] *See* 18 U.S.C. § 1029, 18 U.S.C. § 1362, 18 U.S.C. § 2510, 18 U.S.C. § 2701, 18 U.S.C. § 3121.

[212] New York has created an Internet Bureau, available at http://www.oag.state.ny.us/internet/internet.html (last visited Feb. 20, 2005), and other states have similar organizations.

[213] Nebraska has also legislated in the area of Internet privacy policies, prohibiting by law "knowingly making a false or misleading statement in a privacy policy, published on the Internet....regarding the use of personal information submitted by members of the public." NEB. REV. STAT. § 87-302 (2005).

[214] Online Privacy Protection Act, CAL. BUS. & PROF. CODE § 22575(a) (2005).

information; (2) identify whether the operator maintains a process for the consumer to modify any of the personally identifiable information which is collected; and (3) describe the process through which the operator notifies consumers of changes to the privacy policy.[215] California law also requires disclosure in certain instances of the breach of an individual's personal information.[216] Any agency that owns or maintains computerized data containing a California resident's unencrypted personal information must disclose the occurrence of a breach in the security of the data that has, or is reasonably believed to have, resulted in the acquisition of the resident's personal information by an unauthorized person.[217] If a breach occurs, the law provides specific actions that the owning or maintaining agency must endeavor to disclose to the effected resident.[218] The disclosure requirement applies regardless of whether the personal information is stored in the state of California.[219]

A. STATE LEGISLATION

In 2003, California passed the "Shine the Light" law regarding UCE.[220] Although passed in 2003, it went into effect on January 1, 2005. The bill grants California residents the right to ask businesses with whom they have an "established business relationship" to disclose (1) what type of personal information they have shared with other companies for direct marketing purposes in the preceding calendar year, and (2) the identity of the other companies with whom the information has been shared.[221] "Personal information" is broadly defined, so as to include a range of information from social security numbers to height and weight.[222]

---

[215] Privacy Protection Act, CAL. BUS. & PROF. CODE § 22575(b) (2005).

[216] CAL. CIV. CODE § 1798.29 (2005).

[217] § 1798.29(a).

[218] § 1798.29(g).

[219] § 1798.29(a).

[220] Shine the Light, CAL. CIV. CODE § 1798.83 (2005).

[221] § 1798.83(a).

[222] § 1798.83(e).

Notably, businesses with customers who are California residents are likely to be subject to the law's requirements. The term "established business relationship" encompasses voluntary two-way communication between a business and customer regardless of whether there has been a purchase.[223] The relationship is ongoing until express termination or other specified circumstances.[224]

Particular businesses may be exempt from the law, including businesses with 20 or fewer employees, nonprofit organizations, politicians and other political fundraising groups, banks and financial institutions subject to California financial law, and any business that presents California customers the opportunity to reject the sale of their personal information, either via an opt-in or opt-out provision.[225]

Businesses that are subject to the law must designate a mailing address, electronic or physical, or telephone or fax number, to which customers may deliver their requests.[226] Additionally, the business must choose at least one of the following options: (1) notify employees in contact with customers of the designated means to inquire about the business's privacy practices or compliance; and/or (2) add to the home page a link titled "Your Privacy Rights," connecting the customer to a page describing his rights pursuant to this statute; and/or (3) make the designated address or number readily available upon customer request at every place of business in California where regular customer contact occurs.[227]

Private customers injured by a violation of the "Shine the Light" provision are entitled to bring a civil action.[228] They may recover damages up to a statutorily specified amount, and receive compensation for attorney fees. Further, the violating business may be enjoined from particular conduct.[229]

Also at the state level, a bill was proposed in the Pennsylvania Senate which would amend the state's deceptive and fraudulent

---

[223] § 1798.83(e)(5).

[224] § 1798.83(e)(5).

[225] Shine the Light, CAL. CIV. CODE § 1798.83(c)(1) (2005).

[226] § 1798.83(b).

[227] § 1798.83(b)(A)-(C).

[228] § 1798.84(b).

[229] § 1798.84(c)-(g).

business practices statutes to include a prohibition on false or misleading statements contained in privacy policies published on websites.[230]

B. FEDERAL LITIGATION

The FTC settled multiple actions for wrongdoing related to Internet privacy. The allegations in the FTC actions all relate to corporate information security.

The FTC brought charges against Tower Direct, alleging that a security flaw in Tower's web site exposed customers' personal information to other Internet users, a violation of both federal law and Tower's representations made in its privacy policy.[231] Tower's privacy policy assured customers that only Tower would have access to their personal information, as personal information was password protected with state of the art technology.[232] The FTC alleged that upon redesigning its website, Tower introduced a security vulnerability which gave web users access to certain customer information. The FTC maintained that the security flaw was easy both to prevent and fix. In addition, the FTC claimed that Tower failed to implement checks and controls in the web development process, failed to implement testing policies for the website, and did not provide appropriate employee training and oversight.[233] Because of the security flaw, the assurances made in Tower's privacy policy were false and thereby in violation of Section 5.

After allowing for public comment, the FTC accepted the consent agreement with Tower.[234] The agreement requires Tower to establish, maintain and have certified a comprehensive information security

---

[230] S.B. 705, 2004 Leg. Reg. Sess. (Pa. 2004) (re-reported Nov. 20, 2004), *available at* http://www.legis.state.pa.us/WU01/LI/BI/BT/2003/0/SB0705P2001.HTM.

[231] Complaint, in re Matter of Tower Direct, *at* http://www.ftc.gov/os/caselist/0323209/040421comp0323209.pdf (last visited Feb. 20, 2005).

[232] *Id.*

[233] *Id.*

[234] Consent Agreement, In the Matter of Tower Direct, FTC (filed May 28, 2004) *at* http://www.ftc.gov/os/caselist/0323209/040602do0323209.pdf.

program.[235] It further prohibits Tower from misrepresenting the level of privacy and security it affords customers' personal information.[236]

In another case addressing website security flaws, the FTC brought charges against Petco Animal Supplies for violation of both its website's privacy promises and federal law.[237] Petco made the following security claim on its website: "At Petco.com, protecting your information is our number one priority, and your personal data is strictly shielded from unauthorized access."[238] The site further claimed that "entering your credit card number via our secure server is completely safe. The server encrypts all of your information; no one except you can access it."[239] The FTC alleged that Petco.com was vulnerable to commonly known or reasonably foreseeable attacks that would allow an attacker to gain access to database tables containing consumer credit card information.[240] The FTC charged that the representations of security set forth in Petco's privacy policy were false and misleading and such misrepresentations constitute deceptive acts or practices in violation of Section 5.[241]

Following public comment, the FTC agreed to a consent order with Petco.[242] The consent order requires Petco to establish, maintain, and audit a comprehensive information security program to protect the integrity and security of consumers' personal information.[243] The settlement further bars Petco from misrepresenting the level of protection afforded consumers' personal information.[244]

---

[235] *Id.*

[236] *Id.*

[237] Complaint, In the Matter of Petco Animal Supplies, FTC, *at* http://www.ftc.gov/os/caselist/0323221/041108comp0323221.pdf (last visited Feb. 20, 2005).

[238] *Id.* at 2.

[239] *Id.*

[240] *Id.* at 3.

[241] *Id.* at 4.

[242] Consent Order, In the Matter of Petco Animal Supplies, FTC, *available at* http://www.ftc.gov/os/caselist/0323221/041108agree0323221.pdf (last visited Feb. 20, 2005).

[243] *Id.* at 3, 4.

[244] *Id.* at 3.

In the first FTC case challenging deceptive and unfair practices regarding a company's material change to its privacy policy, the FTC raised charges against Gateway Learning.[245] Gateway Learning used a website to market its "Hooked on Phonics" learning product. The site's privacy policy stated, "We do not sell, rent or loan [sic] any personally identifiable information regarding our consumers with any third party unless we receive customer's explicit consent," and "we do not provide any personally identifiable information about children under 13 years of age to any third party for any purpose whatsoever."[246] The FTC alleged that Gateway Learning rented consumer's personal information, including age ranges and gender of children, to marketers for the purpose of sending mail and making telemarketing calls.[247] A few months later, Gateway Learning revised its privacy policy posted on the website to indicate that consumers' personal information would periodically be provided to "reputable companies."[248] The FTC charged (1) Gateway Learning's original claims regarding the sale, rental, or loan to third parties of consumers' personal information were false; (2) Gateway Learning's retroactive application of the materially altered privacy policy was an unfair practice; and (9) Gateway Learning's failure to notify consumers of the changed privacy policy was a deceptive practice.[249]

After allowing for public comment, the FTC accepted a consent agreement with Gateway Learning.[250] The settlement bars sharing of personal information collected under the original privacy policy unless the company obtains affirmative consent, prohibits the misrepresentation of Gateway Learning's use and collection of consumer data, and bars retroactive application of future material changes to the privacy policy without consumer consent.[251]

---

[245] Complaint, In the Matter of Gateway Learning, FTC, *available at* http://www.ftc.gov/os/caselist/0423047/040707cmp0423047.pdf (last visited Feb. 20, 2005).

[246] *Id.* at 2.

[247] *Id.* at 3, 4.

[248] *Id.*

[249] *Id.* at 5, 6.

[250] Consent Agreement, In the Matter of Gateway Learning, FTC, *available at* http://www.ftc.gov/os/caselist/0423047/040917do0423047.pdf (last visited Feb. 20, 2005).

[251] *Id.*

In addition to civil enforcement, 2004 saw a number of criminal actions regarding Internet privacy. Charges were brought against a Florida email company, Snipermail.com, for allegedly hacking into Axciom, a personal information database company, and selling names and personal information contained within its database to advertisers, or using the information to spam according to customer requests.[252] A 144-count indictment was filed which included, among other charges, multiple counts of unauthorized access to a protected computer and two counts of access device fraud.[253]

A software engineer employed by America Online has been charged with stealing millions of email addresses from AOL's subscriber list and subsequently selling them to an intermediary.[254] This intermediary used the emails to promote his own online gambling website and sold the list to spammers.

Three executives from Dallas European Parts Distributors, a Texas car parts distributorship, are alleged to have stolen information and photographs from a competitor's website.[255] The indictment includes allegations of computer password trafficking as well as unauthorized access to a protected computer.[256] The executives are alleged to have illegally obtained usernames and passwords for the competitor's website and then to have used them to gain commercial advantages over the company.[257]

C. STATE LITIGATION

At the state level, New York was the site of two agreements regarding corporate Internet privacy practices. The New York attorney general's office reached an agreement with Barnes & Noble to address its privacy and information security practices. The Barnes & Noble website contained a design flaw which granted unauthorized access to consumers' personal information and allowed users to use

---

[252] United States v. Levine, No. 4:04CR00175 (E.D. Ark. filed July 21, 2004).

[253] *Id.*

[254] United States v. Smathers, No. 1:04-MJ-01224-UA (S.D. N.Y. filed June 24, 2004).

[255] United States v. Rowghani, No. CR-04-0011 (N.D. Cal. filed Feb. 9, 2004).

[256] *Id.*

[257] *Id.*

other consumers' accounts to make purchases on the site.[258] The agreement called for Barnes & Noble to implement an information security program, establish employee oversight and training programs, hire an external auditor, and pay a fine.[259]

The New York attorney general's office also reached an agreement with PayPal regarding disclosure of the rights of account holders upon failure of an affiliated merchant to deliver merchandise.[260] PayPal's User Agreement stated that it afforded its account holders "the rights and privileges expected of a credit card transaction" when in practice consumers were not granted such rights.[261] The agreement requires PayPal to clarify the account holder's rights in the User Agreement as well as pay a penalty.[262]

D. CONCLUSION

The prevention and prosecution of fraud and wrongdoing will remain a pertinent issue. Privacy policies remain an integral component to ensuring consumer protection and changing technology dictates that security vulnerabilities will be an ever-present threat to privacy. In a society increasingly dependent on technology and the Internet, corporations will need to maintain vigilance with regard to their customers' personal information and the policies and practices they implement to protect that personal information.

VII. EMAIL AND INTERNET ACTIVITY: CONTEMPORANEOUSLY MONITORING OF ACTIVITY BY PRIVATE ACTORS AND THE GOVERNMENT

The Fourth Amendment provides for freedom "against unreasonable searches and seizures" by the government without "probable cause."[263] In terms of electronic communications, those

---

[258] Press Release, N.Y. Att'y Gen. Off., Attorney General Reaches Agreement with Barnes and Noble on Privacy and Security Standards (Apr. 29, 2004).

[259] *Id.*

[260] Press Release, N.Y. Att'y Gen. Off., PayPal to Clarify Disclosures Related to Rights for Undelivered Goods (Mar. 8, 2004).

[261] *Id.*

[262] *Id.*

[263] U.S. CONST. amend. IV.

protections have been extended to private actors by the Electronic Communications Privacy Act ("ECPA").[264] Although the protections have been extended, they do not quite parallel the protections under the Fourth Amendment, providing for exceptions to the protections and thresholds that are sometimes lower than the high "probable cause" required by the Fourth Amendment.[265]

One of the areas of change in 2004 was that email providers significantly increased the amount of storage available to users. For example, GMail entered the market and offered users 1 gigabyte of storage space for email, advertising that the user would never need to delete email again.[266] This is notable because Title II of ECPA, the Stored Communications Act ("SCA"), makes distinctions between opened and unopened electronic messages and electronic messages left on a server for more than 180 days.[267] Only unopened electronic messages that are less than 180 days old require probable cause for law enforcement access.[268] If the email is opened and left on the third-party server or unopened for more than 180 days, the government need only obtain an "administrative subpoena[,] ... grand jury or trial subpoena[, or] ... court order" to access the electronic message.[269]

This is not the only area of ECPA that has recently been highlighted. The *United States v. Councilman* decision explores the edges of the Wiretap Act and the definition of contemporaneous access while markedly avoiding the question of whether there was a violation of the SCA.[270] Another case discussed ECPA and whether evidence

---

[264] The Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848 (1999) consists of two titles: Title I ("the Wiretap Act") 18 U.S.C. §§ 2510-22 and Title II ("the Stored Communications Act") 18 U.S.C. §§ 2701-11.

[265] *See generally Current Legal Standards for Access to Papers, Records, and Communications: What Information Can the Government Get About You, and How Can They Get It?*, THE CENTER FOR DEMOCRACY AND TECHNOLOGY (July 2004), *at* http://www.cdt.org/wiretap/govaccess/govaccesschart-11x17.pdf.

[266] *GMail still dogged by privacy issues*, COMPUTERWEEKLY.COM (Apr. 16, 2004), *available at* http://www.computerweekly.com/articles/article.asp?liArticleID=129948&liFlavourID=1&sp=1.

[267] Stored Communications Act, 18 U.S.C. § 2703 (2002).

[268] *Id.*

[269] § 2703(b)(1)(B).

[270] *See* United States v. Councilman, 373 F.3d 197, 198 (1st Cir. 2004), *rehearing en banc granted*, 385 F.3d 793 (2004).

obtained by spyware was improperly obtained in violation of state wiretap laws.[271]

A. FEDERAL LITIGATION

The federal circuit courts are starting to develop new case law interpreting ECPA, and determining whether accessing an electronic communication falls under the Wiretap Act or the Stored Communications Act. One of these cases was *Theofel v. Farey-Jones*, where the court held that the Internet Service Provider ("ISP") did not violate the Wiretap Act by accessing messages on its servers.[272] Specifically, the court found that the messages were in electronic storage because "prior access is irrelevant to whether the messages at issue were in electronic storage."[273] Consequently, the ISP did not violate the Wiretap Act because "Congress did not intend for intercept to apply to electronic communications when those communications are in electronic storage."[274] In its opinion, accessing stored but unopened electronic message was not an "acquisition contemporaneous with transmission."[275]

Another interpretation was proffered by the First Circuit in *United States v. Councilman*, in which the court held that an ISP that primarily dealt in rare books did not violate the Wiretap Act by scanning inbound emails from Amazon.com to its customers.[276] The ISP essentially offered comparative advertising on books sold by Amazon.com to itself, a rare books dealer.[277] Here, the court noted that "[t]he Wiretap Act's purpose was, and continues to be, to protect the privacy of communications."[278] Further, it believed "that the language of the statute makes clear that Congress meant to give lesser

---

[271] *O'Brien*, *supra* note 55, at *4-5.

[272] Theofel v. Farey-Jones, 359 F.3d 1066, 1077 (9th Cir. 2004), *cert. denied*, 125 S. Ct. 48 (2004).

[273] *Id.* at 1077.

[274] *Id.* (quotation marks removed).

[275] *Id.*

[276] *Councilman*, 373 F.3d at 199-200.

[277] *Id.*

[278] *Id.* at 203.

protection to electronic communications than wire and oral communications" and that "at this juncture, much of the protection may have been eviscerated by the realities of modern technology."[279] With this in mind, the court found no violation of the Wiretap Act, although it did not rule on whether there was a violation of the Stored Communications Act.[280]

The dissenting judge in *Councilman* discussed how "[t]he privacy protections established by the Stored Communications Act were intended to apply to two categories of communications: 'those associated with transmission and *incident thereto*' and those of 'a back-up variety.'"[281] He went on to conclude that "[t]he first category refers to temporary storage ... [and that] this category does not include messages that are still in transmission, which remain covered by the Wiretap Act."[282] In other words, "the Wiretap Act would apply to messages that are intercepted contemporaneously with their transmission[,] and the Stored Communications Act would apply to messages that are accessed non-contemporaneously with transmission."[283] Protection from interception contemporaneous with transmission is important because "[t]he Stored Communications Act does not contain any of the Wiretap Act's special protections."[284] With the majority's decision finding that temporary storage of electronic messages in locations incident to transmission was sufficient to preempt the contemporaneous requirement, "[a] federal law enforcement agent could obtain access to such communications simply by obtaining a warrant."[285]

In an area related to wiretapping, the Sixth Circuit will hear a case to determine whether an Internet Protocol ("IP") address is personally identifiable information ("PII").[286] In *Klimas v. Comcast Corp.*, the

---

[279] *Id.* at 203-04

[280] *Id.* at 204.

[281] *Councilman*, 373 F.3d at 207 (Lipez, J., dissenting) (emphasis added).

[282] *Id.* (Lipez, J., dissenting).

[283] *Id.* at 208 (Lipez, J., dissenting).

[284] *Id.* (Lipez, J., dissenting).

[285] *Id.* (Lipez, J., dissenting).

[286] Klimas v. Comcast Corp., 2003 WL 23472182, at *5 (E.D. Mich. 2003), *appeal not yet docketed*; *see also IP Address 'Personally Identifiable Info,' 6th Cir. Told*, 1 No. 9 ANDREWS PRIVACY LITIG. REP. 3 (May 24, 2004).

district court found that "a dynamic IP address cannot constitute PII."[287] This is so because, "[u]nlike a subscriber's name, address, social security number, etc., a dynamic IP address is constantly changing."[288] The district court went on to state: "[t]he fact that Comcast may have had the power to make such a correlation does not render the information collected PII."[289] If a dynamic IP address is held to be PII, it can likely be excluded from Federal requests for the Internet equivalent of Pen Registers and Trap and Trace Devices.[290]

B. FEDERAL LEGISLATION

Partially in response to the *Councilman* decision from the First Circuit, the 108th Congress considered a variety of bills to clarify that accessing undelivered email was a contemporaneous access that provided for the possibility of violating the Wiretap Act or otherwise specifying that it did not agree with the *Councilman* decision; none of them were enacted.[291]

C. STATE LEGISLATION

In 2004, California passed the Employee E-Mail Protection Bill, which required businesses to inform employees if the business planned

---

[287] *Id.*

[288] *Id.*

[289] *Id.*

[290] *See Approvals for Federal Pen Registers and Trap and Trace Devices 1987-1998,* EPIC (Sept. 13, 2004) (defining a pen register as "an electronic device which records all numbers dialed from a particular phone line" and a trap and trace device as a device that "records the originating phone numbers of all incoming calls on a particular phone line" – in other words, devices that capture envelope and routing information and not personally identifiable information), *at* http://www.epic.org/privacy/wiretap/stats/penreg.html.

[291] *See Email Privacy Act of 2004*, H.R. 4956, 108th Cong. (2004), *available at* http://thomas.loc.gov/cgi-bin/bdquery/z?d108:hr4956:; *see also Email Privacy Protection Act of 2004*, H.R. 4977, 108th Cong. (2004), *available at* http://thomas.loc.gov/cgi-bin/bdquery/z?d108:hr4977:. *See generally 2004 United States v. Councilman email privacy case*, THE CENTER FOR DEMOCRACY AND TECHNOLOGY, *at* http://www.cdt.org/wiretap/ councilman.shtml (last visited March 13, 2005).

to monitor the employees' emails or Internet usage. Governor Schwarzenegger vetoed the bill.[292]

D. PRIVATE ACTIONS

Because the Fourth Amendment only applies to state actions, employers have a lot of leeway with what employee information they can access while their employees are at work.[293] This fact has led to some newsworthy incidents. For example, a Delta Air Line employee was fired in November 2004 for maintaining a web log ("blog") that included pictures of her performing non-work-related activities while at work.[294] In addition to reading publicly posted messages from employees, employers are also allowed to read and monitor an employee's email and Internet usage while at work, with 44% of large corporations even going so far as to hire employees whose job it is to read other employees' emails.[295]

E. INTERNATIONAL

There are privacy laws in more jurisdictions that just the United States; some of them have similar quirks, however. For example, the New South Wales government in Australia is "moving to outlaw bosses spying on workers' emails," absent a court order.[296] Also, other

---

[292] *See* Employee E-Mail Protection Bill, S.B. 1841 (Cal. 2004); *see also California Assembly approves employee e-mail protection*, THE ASSOCIATED PRESS (Aug. 17, 2004), *available at* http://www.siliconvalley.com/mld/siliconvalley/news/9424741.htm; *Arnold Vetoes Privacy Bill*, WIRED (Sept. 30, 2004), *available at* http://www.wired.com/news/privacy/0,1848,65152,00.html.

[293] *See* U.S. CONST. amend. IV.

[294] *Blog-linked firings prompt calls for better policies*, CNN (Mar. 6, 2005), *at* http://www.cnn.com/2005/TECH/internet/03/06/firedforblogging.ap/; *see also Companies That Have Fired People for Blogging* (Jan. 9, 2005) (listing a number of companies alleged to have fired people due to blogging, including Delta Air Lines and Starbucks Coffee), *at* http://www.boingboing.net/2005/01/09/companies_that_have_.html.

[295] Jo Best, *Companies step up e-mail surveillance*, ZDNET NEWS (July 20, 2004), *at* http://news.zdnet.com/2100-1009_22-5276512.html.

[296] *NSW targets employers' email snooping*, ABC NEWS (Mar. 30, 2004), *at* http://www.abc.net.au/news/newsitems/s1077250.htm; *see also* Press Release, Australian Democrats, Democrats to Oppose E-mail and SMS Spy Laws (Nov. 29, 2004) (Australian Democrats press release opposing a move "to increase police powers to access private SMS, email and voicemail messages without a telecommunications interception warrant."), *available at* http://www.democrats.org.au/news/index.htm?press_id=4276&display=1.

countries are eyeing global services offered by U.S. companies, with a prime example that some in Europe feel Google's GMail may violate European privacy laws, because it scans the contents of email and provides targeted advertising.[297]

F. CONCLUSION

There has been a great deal of action and surprise from various privacy groups over decisions like *Councilman*, where the court literally interpreted ECPA to find no violation of the Wiretap Act. Similarly, there is a laissez-faire attitude in the U.S. regarding an employer's ability to monitor an employee's email and Internet usage, both at work and at home, if the Delta Air Line blog incident is any indication. It is certainly possible that a trend is forming where Internet-based communications are becoming both more popular and less protected. This dichotomy will likely be further highlighted in the ongoing Voice over Internet Protocol and wiretapping debate.[298]

VIII. EMAIL AND INTERNET ACTIVITY: SUBSEQUENT ACCESS TO RECORDS BY PRIVATE ACTORS AND/OR THE GOVERNMENT

Accessing the records and results of email and Internet activity after it has transpired is closely related to accessing email and Internet activity contemporaneously. This topic focuses on the use of customer lists, specifically with respect to identity theft, under the subpoena provisions of the USA PATRIOT Act, and in connection to the peer-to-peer ("P2P") file-sharing lawsuits.[299] Further, with identity theft increasingly in the forefront, the security of information databases has become an increasingly important concern.

---

[297] *See UK lobby says Google mail may violate privacy laws*, REUTERS (Apr. 5, 2004), *at* http://www.forbes.com/home_europe/newswire/2004/04/05/rtr1323420.html; *see also Germans garotte Google Gmail over privacy*, THE REGISTER (Apr. 8, 2004), *at* http://www.theregister.co.uk/2004/04/08/gmail_germany/.

[298] The 2004 debate over the wiretapping of Voice over Internet Protocol ("VoIP") communications was intentionally omitted from this paper. Please see the piece written be John Morris elsewhere in this issue of *I/S* for further reading.

[299] An employer's right to access employee information was discussed briefly in the previous subsection.

A. STATE LEGISLATION

Many states are just starting to look into information security. For example, Utah passed a Master Study Resolution, one of the points of which was "to study the disclosure of personally identifiable information by an Internet business and the importance of ensuring privacy."[300] California implemented a law that goes a step further: All Internet-based companies collecting personally identifiable information from California residents need to post and adhere to a privacy policy.[301] In light of a study that found that "Internet companies can boost sales and build trust with online shoppers by providing clear and readily available privacy disclosures," other states may very well implement laws similar to California's, mandating privacy policies.[302] Not everyone agrees that mandating on-line privacy statements is a good policy, however, with some citing concerns about "increases in the cost of doing business online."[303]

---

[300] *Master Study Resolution*, SJR 0010 (Utah 2004), *at* http://www.le.state.ut.us/~2004/bills/sbillenr/sjr010.htm.

[301] *Online Privacy Protection Act*, CAL. BUS. & PROF. CODE §§ 22575-22579 (2003) (effective July 1, 2004), *available at* http://www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=22001-23000&file=22575-22579 (last visited Mar. 14, 2005); *see also California Online Privacy Protection Act (OPPA)*, WATCHFIRE (advertising solutions to help bring companies into compliance with the *Online Privacy Protection Act* and detailing the requirements for compliance), *available at* http://www.watchfire.com/legislation/oppa.aspx (last visited Mar. 14, 2005); *Privacy guidelines for Irish web sites*, OUT-LAW.COM (Sept. 14, 2004) (reporting that "Ireland's Data Protection Commissioner has published Guidelines for the content and use of privacy statements on web sites to help businesses comply with the country's rules on data protection."), *at* http://www.out-law.com/php/page.php?page_id=privacyguidelinesf1095350907.

[302] *See* Press Release, U. of Cal. Irving, Clear privacy practices boost trust and online sales for Internet companies, determines UCI study (Aug. 30, 2004), *available at* http://today.uci.edu/news/release_detail.asp?key=1208; *see also* Daniel Thomas, *P&G privacy plan tackles data laws*, PC MAGAZINE (Dec. 2, 2004) (discussing Proctor & Gamble's "plans to introduce privacy monitoring software worldwide to deal with varying information laws"), *available at* http://www.pcmag.co.uk/news/1159792.

[303] *California Online Privacy Protection Act of 2003: Good Practice, Bad Precedent*, ENTREPRENEURS BLOG (June 4, 2004), *at* http://entrepreneurs.about.com/od/internetmarketing/i/caprivacyact.htm.

B. FEDERAL LITIGATION: GOVERNMENT SUBPOENAS

One area of interest in 2004 was a lawsuit brought by an anonymous Internet Service Provider and the American Civil Liberties Union.[304] A federal district court found portions of 18 U.S.C. § 2709 unconstitutional.[305] These portions were a section of the Stored Communications Act that provided the FBI access to stored information through use of a National Security Letter ("NSL") as amended by the USA PATRIOT Act.[306] In its conclusion, the court stated that:

> the compulsory, secret, and unreviewable production of information required by the FBI's application of 18 U.S.C. § 2709 violates the Fourth Amendment, and that the non-disclosure provision of 18 U.S.C. § 2709(c) violates the First Amendment. The Government is therefore enjoined from issuing NSLs under § 2709 or from enforcing the non-disclosure provision in this or any other case....[307]

In other words, lack of notice and prohibition of discussing the requests under the NSL violated both the Fourth and First Amendments. Perhaps appropriately, one writer described NSLs as where, "[i]n true Gestapo style, the recipient of such a letter is forbidden to disclose the fact that a demand for information has been made."[308] Enforcement of this ruling is stayed until the appeal is heard.[309]

In another case of government access to information in the post-September 11, 2001 era, the court in the lawsuit against Northwest Airlines found "a 'privacy policy' published on an airline's website"

---

[304] *See* Doe v. Ashcroft, 334 F. Supp. 2d 471, 526-27 (S.D.N.Y. 2004).

[305] *Id.*

[306] *Id.*

[307] *Id.* (footnotes omitted); *see* Press Release, American Civil Liberties Union, In ACLU Case, Federal Court Strikes Down Patriot Act Surveillance Power As Unconstitutional (Sept. 29, 2004), *at* http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=16603&c=282.

[308] Thomas Greene, *US judge raises bar on net privacy*, THE REGISTER (Sept. 30, 2004), *at* http://www.theregister.co.uk/2004/09/30/patriot_act_judged/.

[309] *See* Doe v. Ashcroft, 334 F. Supp. 2d at 527.

does not interfere "with the carrier's ability to share information with the government" because "Northwest's privacy policy did not mislead its customers ... and that by sharing passenger data with NASA for noncommercial research purposes Northwest did not violate the express or intended meaning of that policy."[310] Contemporaneously in 2004, the European Parliament "asked the European Court of Justice to reject an [European Union - United States] treaty that would allow authorities to collect air passengers' personal data and pass them on to the US."[311] This request was made "because of privacy concerns, but EU governments proceeded with it regardless."[312] Finally, the Platform for Privacy Preferences ("P3P") Project is continuing to gain steam, with one news article reporting that more government websites are implementing machine-readable privacy policies.[313]

In a final government subpoena case that does not necessarily fall under the umbrella of peer-to-peer file-sharing, America Online lost on summary judgment when one of its employees divulged a customer's subscriber information in violation of Title II of ECPA, the Stored Communications Act ("SCA").[314] This was the outcome, notwithstanding the fact that the AOL employee acted in response to an ultimately invalid warrant requesting the information:

> In sum, therefore, while the legal invalidity of the warrant is an element of an ECPA violation, it is not one of the factual circumstances [that the employee] must have known to have "knowingly divulge[d]" the information to the ... police. To conclude otherwise would render the ECPA impotent to reach a wide variety of circumstances where the legal

---

[310] EPIC v. Northwest Airlines, 2004 WL 2049588, at *8, at *13-14 (D.O.T. Sept. 10 2004) (unpublished opinion); *see generally, Northwest Airlines' Disclosure of Passenger Data to Federal Agencies*, EPIC (Sept. 20, 2004), *at* http://www.epic.org/privacy/airtravel/nasa/.

[311] *Privacy concerns over EU-US treaty*, RTE NEWS (June 25, 2004), *at* http://www.rte.ie/news/2004/0625/eu.html.

[312] *Id.*

[313] Machine readable privacy policies mean that consumers will be able to set their privacy preferences in their Internet browser, and the browser will, for example, alert them when it finds a site that purports to follow data policies in line with the consumers' beliefs. *Federal Agencies Slow to Meet Online Privacy Criteria*, FCW.COM (Apr. 27, 2004), *at* http://www.usatoday.com/tech/news/internetprivacy/2004-04-27-privacy-criteria_x.htm; *see also P3P Public Overview*, W3C, *at* http://www.w3.org/P3P/ (last visited Mar. 15, 2005).

[314] Freedman v. America Online, 329 F. Supp. 2d 745, 747 (E.D. Va. 2004).

> invalidity of a warrant is more apparent or more subtle than it was here.[315]

Therefore, the court found that the act of divulging information was enough to uphold summary judgment against America Online, regardless of the validity of the warrant.[316]

C. FEDERAL LITIGATION: PEER-TO-PEER FILE-SHARING

Peer-to-peer ("P2P") file-sharing was a hot button topic in 2004. There were a plethora of suits launched by the Recording Industry Association of America and other content creators against various groups in an attempt to stymie the torrential flow of music and software piracy through P2P exchanges.[317] The trouble with P2P file-sharing is that it is difficult to ascertain exactly who has committed the copyright infringement. This issue has been the focus of much of the initial litigation.

One of the first unsuccessful tactics employed by the copyright holders was attempting to subpoena the Internet Service Providers ("ISPs") under the Digital Millennium Copyright Act.[318] From there, the content companies utilized another approach, suing groups of

---

[315] *Id.* at 749.

[316] *Id.* at 751.

[317] The focus of this section is on privacy issues related to P2P file-sharing. Cases such as MGM Studios v. Grokster, 380 F.3d 1154, 1157 (9th Cir. 2004), *cert. granted*, 125 S. Ct. 686 (2004) (appeal pending before the U.S. Supreme Court, concluding that "the defendants [who provide P2P software] are not liable for contributory and vicarious copyright infringement and affirm[ing] the district court's partial grant of summary judgment") or *The Induce Act*, S. 2560, 108th Cong. (2004), *available at* http://thomas.loc.gov/cgi-bin/query/z?c108:S.2560:, *commentary, available at* http://www.siliconvalley.com/mld/siliconvalley/business/columnists/9607090.htm (last visited March 15, 2005), although interesting, do not directly relate to the subpoenaing of customer information or other privacy-related issues and will not be discussed beyond this footnote.

[318] *See* Recording Industry Association of America v. Verizon Internet Services, 351 F.3d 1229, 1231 (D.C. Cir. 2003), *cert. denied*, 125 S. Ct. 309 (2004); *see also* Verizon Internet Services v. Recording Industry Association of America, 351 F.3d 1229, 1231 (D.C. Cir. 2003), *cert. denied*, 125 S. Ct. 347 (2004) (cross-petitioner claim); *see also In re* Charter Communications, 393 F.3d 771, 776 (8th Cir. 2005) (agreeing with the holding from the D.C. Circuit, barring copyright owners from subpoenaing customer information under the Digital Millennium Copyright Act from ISPs who "merely acts as a conduit" between two Internet users.); *see also* BMG Canada v. Doe, [2004] F.C. 488 (reaching a similar conclusion under Canadian law), *at* http://news.findlaw.com/hdocs/docs/cyberlaw/criadoe33104opn.pdf.

specific but unidentified "John Does."[319] Generally, without further showing that the claims are similar, such as conspiring to operate a peer-to-peer file-sharing network, joinder has been found to be inappropriate.[320] However, if there is only one John Doe or the court decides to allow prosecution of the first John Doe, discovery has been allowed, compelling the ISPs to turn over customer information.[321]

D. STATE LITIGATION

Most of the state litigation focuses around Internet-based businesses accessing and potentially misusing customer information. There are some seemingly straightforward cases where businesses have sold personally identifiable information to others who have misused it or misused it themselves.[322]

---

[319] *See* BMG Music v. Does 1-203, 2004 WL 953888, at *1 (E.D. Pa 2004) (unpublished opinion finding that plaintiffs were "improperly joined" because BMG attempted "to bring over two-hundred factually distinct actions in one lawsuit" and, therefore, denying request to expedite discovery of the Does' identities by compelling Comcast's assistance.); *see also* Anita Ramasastry, *Court strikes a good balance in file swapping case,* CNN (Nov. 11, 2004) (discussing the notice requirements to the defendants in "John Doe" file-sharing lawsuits), *at* http://www.cnn.com/2004/LAW/11/11/ramasastry.file.swapping/.

[320] *Id.; but also Judges Allow Movie Studios to Seek IDs for Server Operators,* 22 NO. 15 ANDREWS COMPUTER & INTERNET LITIG. REP. 5 (Dec. 28, 2004) (discussing the results of two federal district court rulings allowing "motion picture companies to obtain the identities of several 'John Doe' defendants who are accused of operating a peer-to-peer file sharing system that allows individuals to download movies." (Columbia Pictures Industries Inc. et al. v. Does, No. 8:04-cv-2697-T-17TBM (M.D. Fla. 2004) and Disney Enterprises Inc. et al. v. Does, No. 8:04-cv-2698-T-24MAP (M.D. Fla. 2004))).

[321] *See* Twentieth Century Fox Film Corp. v. Does 1-12, 2004 WL 3241669, slip op. at *1 (N.D. Cal. 2004) (finding improper joinder of Does 2-12 but holding, until plaintiffs can show that this case should be treated differently, it will be stayed "[e]arly discovery as to Doe 1" because "good cause [was] shown" from "Pacific Bell Internet."), *available at* http://www.eff.org/IP/P2P/MPAA_v_ThePeople/20041123_20thv12_order_severing_cases.pdf.

[322] *See, e.g.,* Holly Ramer, *Mother of slain woman settles lawsuit against info-broker,* THE ASSOCIATED PRESS (March 10, 2004) (where "[a]n Internet information broker has agreed to pay $85,000 to a ... woman who sued ... over her daughter's killing" when the company sold the eventual murderer, "who chronicled his obsession with [the victim] and his plot to kill her on a Web site ... her Social Security number and other information, including her work address" for $150. According to the article, in 2003, "the [New Hampshire] Supreme Court ruled ... that private investigators or information brokers have legal obligations to people whose information it sells."), *at* http://www.usatoday.com/tech/news/internetprivacy/2004-03-10-boyer-suit-settled_x.htm; *see also, e.g.,* Press Release, Dep't of Justice, Malibu Man Sentenced to 11¼ Years in Federal Prison in $37 Million Internet Credit Card Fraud Scheme (May 10, 2004) (press release commenting on prolonged litigation where the operator of

E. CONCLUSION

As the businesses in the United States and worldwide continue to retain customer data, they may be subjected to greater demands or temptations to access the data for purposes other than that for which it was originally collected. Although there appear to be some limits on the subpoena power of the U.S. government, where some subpoenas still require that the standards of due process be met, the government is generally able to access the data. Private companies, however, are facing pressure to create and enforce privacy policies, along with more severe penalties for violating those policies. Some individual states may be attempting to bring businesses serving their residents in line with a more European approach: collecting only the data necessary and using it only for the purposes prescribed in the privacy policy.

IX. CHILD ONLINE PROTECTION

In 2004, a large amount of legislation and litigation was focused on the protection of children against unwanted content on the Internet. The foundation for protecting children online at the federal level is the Child Online Privacy Protection Act ("COPPA").[323] COPPA is applicable to: operators of commercial websites or online services directed to children less than 13 years of age that collect personal information from children, operators of general audience websites that have actual knowledge that personal information from children is being collected, and operators of general audience websites that have a separate children's area and collect children's personal information.[324]

COPPA mandates that operators meet several requirements to achieve compliance. These requirements include: posting a privacy policy on the website providing notice of what personal information is collected;[325] obtaining verifiable parental consent prior to the collection, use, and/or disclosure of children's personal information,

---

Internet pornography business was sentenced for using stolen credit cards), *available at* http://www.usdoj.gov/usao/cac/pr2004/068.html.

[323] Child Online Privacy Protection Act, 15 U.S.C. §§ 6501-06.

[324] Children's Online Privacy Protection Rule, 16 C.F.R. § 312.2, 312.3; *see also You, Your Privacy Policy and COPPA*, FTC (publication) *available at* http://www.ftc.gov/bcp/conline/pubs/buspubs/coppakit.pdf (last visited Feb. 20, 2005).

[325] 16 C.F.R. § 312.4(b).

with some exceptions;[326] giving an option for parental consent to the collection and use of personal information from their children as well as a right to refuse its use or maintenance;[327] not conditioning a child's participation in a game or activity on the further disclosure of personal information beyond what is necessary to reasonably participate;[328] and establishing and maintaining reasonable procedures protecting the confidentiality, security, and integrity of the personal information collected from children.[329]

The regulations provide for exceptions whereby an operator is permitted to collect a child's email address without first obtaining parental consent.[330] In addition, the regulations contain a safe harbor provision to allow industry groups or others to establish a self-regulatory program to govern compliance of that group's participants.[331] Enforcement of COPPA falls on the FTC because violations are treated as a violation of a rule defining an unfair or deceptive practice as prescribed in the FTC Act.[332]

Also relevant at the federal level is the Child Online Protection Act ("COPA").[333] Narrower in scope than the aforementioned legislation, COPA seeks to prevent minors from exposure to particular materials on the Internet. The law prohibits knowingly making communication for commercial purposes that is available to any minor which includes any material harmful to minors.[334] Currently, the constitutionality of the statute is at issue.[335]

---

[326] § 312.5.

[327] § 312.6.

[328] § 312.7.

[329] § 312.8.

[330] Children's Online Privacy Protection Rule, 16 C.F.R. § 312.5(c).

[331] § 312.10.

[332] § 312.9.

[333] Child Online Protection Act, 47 U.S.C. § 231.

[334] § 231(a)(1).

[335] *See infra* note 362.

Even narrower than COPA, the Children's Internet Protection Act ("CIPA") applies to public libraries and schools.[336] CIPA requires schools and libraries to enable filters which prevent minors from exposure to on-screen obscenity, child pornography, or other harmful material, as a prerequisite to receiving federal subsidies for Internet access and computer equipment.[337] The constitutionality of this statute was upheld by a divided Supreme Court in 2003.[338] Congress also requires ISPs to notify authorities if an incident of child pornography or exploitation comes to its attention.[339]

States have enacted a variety of laws directed towards protecting minors from Internet related harms. These laws fall under three general categories: child pornography reporting requirements, laws prohibiting the electronic solicitation or luring of minors, and laws addressing filtering and usage policies in schools and libraries.[340] Reporting requirements mandate that computer technicians or ISPs report child pornography encountered within the scope of their employment.[341] Electronic solicitation and luring laws seek to prevent minors from being induced to engage in illegal sexual conduct via computers and the Internet.[342] State filtering laws generally require

---

[336] Children's Internet Protection Act, Pub. L. No. 106-554, 114 Stat. 2763A-335 (2000) (codified at 20 U.S.C. § 9134(f) (2000) and 47 U.S.C. § 254(h) (2000)).

[337] § 9134(f).

[338] U.S. v. American Library Ass'n, 539 U.S. 194 (2003).

[339] 42 U.S.C. § 13032 (2003).

[340] *Children & The Internet: Laws and Legislation*, National Conference of State Legislatures, *at* http://www.ncsl.org/programs/lis/kidnet/laws.htm (Mar. 13, 2005).

[341] ARK. CODE ANN. § 5-27-604; MICH. PEN. CODE § 750.145c(9); MO. REV. STAT. § 568.110.1; S.C. CODE ANN. § 16.3.850; S.D. CODIFIED LAWS § 22-22-24.18.

[342] ALA. CODE § 13A-6-110-111; ARK. CODE ANN. § 5-27-603; CAL. PENAL CODE § 288.2; COLO. REV. STAT. § 13-21-1002; CONN. GEN. STAT. § 53a-90a; DEL. CODE. ANN. tit. 11 § 1112A; FLA. STAT. ch. 847.0135; GA. CODE ANN. § 16-12-100.2; HAW. REV. STAT. § 707.756-.757; IDAHO CODE § 18-1509A; 720 ILL. COMP. STAT. 5/11-6; IND. CODE § 35-42-4-6; ME. REV. STAT. ANN. tit. 17-A, § 259; MD. CODE ANN., CRIM. LAW § 11-207; MICH. COMP. LAWS § 750.145c-d; MINN. STAT. § 609.352; MISS. CODE ANN. § 97-5-27; MO. REV. STAT. § 566.151; NEB. REV. STAT. § 28-320-02; NEV. REV. STAT. § 201.560, 207.260; N.H. REV. STAT. ANN. § 649-B:3, 649-B:4; N.J. STAT. ANN. § 2C:13-6; N.M. STAT. ANN. § 30-37-3.2(B); N.Y. PENAL LAW § 235.22; N.C. GEN. STAT. § 14-202.3; N.D. CENT. CODE § 12.1-20-05.1; OKLA. STAT. tit. 21, § 1040.13a; S.D. CODIFIED LAWS § 22-22-24.4, 22-22-24.5; TENN. CODE ANN. § 39-13-528; UTAH CODE ANN. § 76-4-401; VT. STAT. ANN. tit. 13, § 2828; VA. CODE ANN. § 18.2-374.3; W. VA. CODE §61-3C-14b; WIS. STAT. § 948.075.

schools and/or libraries to put in to place policies that prevent minors from accessing obscene, sexually explicit, or otherwise harmful materials.[343]

A. FEDERAL LEGISLATION

In March of 2004, Senators Wyden and Stevens introduced the Children's Listbroker Privacy Act.[344] The bill would prohibit corporations from selling children's personally identifiable information for commercial marketing purposes. The bill notes that other statutes, such as COPPA, address the collection and disclosure of children's information, but that data may be collected outside the rubric of these statutes. While the bill does not specifically address Internet privacy issues, its function as a catchall may impact the collection and use of personal information from children obtained online.

B. STATE LEGISLATION

At present, state legislation comparable to the requirements of COPPA is lacking. However, 2004 saw three states introduce bills aimed at protecting children's personal information online. Central to all three legislative endeavors is the creation of a registry of contact points for minors.

The Utah governor signed into law a bill which requires the Division of Consumer Protection to establish a contact points registry for minors.[345] For the purposes of the law, email is considered a contact point. The law prohibits an individual from sending material

---

[343] ARIZ. REV. STAT. § 34-501, 34-502; ARK. CODE ANN. § 6-21-107, 13-2-104; CAL. EDUC. CODE § 18030.5; COLO. REV. STAT. § 24-90-401- 404, 24-90-603, 22-87-101- 107; DEL. CODE ANN. tit. 29 § 6601C-6607C; KY. REV. STAT. ANN. § 156.675; LA. REV. STAT. ANN. 17:100.7; MD. CODE ANN., COM. LAW § 23-506.1; MICH. COMP. LAWS § 397.602, 397.606; MINN. STAT. § 134.5; MO. REV. STAT. §182.825, 182.827; N. H. REV. STAT. ANN. 194:3-d; N.Y. EDUC. LAW § 260(12); 24 PA. CONS. STAT. § 4304; S.D. CODIFIED LAWS § 22-24-55- 59; TEX. EDUC. CODE ANN. § 32.151, 32.152; TEX. GOV'T CODE ANN. § 441.1385; UTAH CODE ANN. § 9-7-213- 217, 53A-3-422- 424; VA. CODE ANN. § 22.1-70.2, 42.1-36.1. Both Ohio and Oklahoma accomplish similar protective goals via uncodified bills. *See* H.B. 215, 122nd Gen. Assem., Reg. Sess. (Oh. 1997); H.C.R. 1097, 45th Leg. (Ok. 1997).

[344] S. 2160, 108th Cong. § 2 (2004).

[345] H.B. 165, 2004 Gen. Sess. (Utah 2004) (codified at UTAH CODE ANN. § 13-39-101, 102, 201, 202, 203, 301, 302, 303, 304).

to a registered contact point which advertises a product or service which the law prohibits the minor from purchasing, or contains or advertises material statutorily defined as harmful to minors.[346]

Michigan enacted a similar law, requiring the Department of Labor and Economic Growth to create a registry of contact points for minors.[347] Again, email is considered a contact point. The law prohibits the sending of a message to a contact point, if the primary purpose of the message is directly or indirectly to advertise a product a service that under the law a minor is prohibited from purchasing, viewing, possessing, participating in, or otherwise receiving.[348]

Georgia has proposed a law similar to the aforementioned statutes; however, it remains in the Georgia House of Representatives.[349]

C. FEDERAL LITIGATION

In February of 2004, the FTC settled charges brought under COPPA against two corporations, Bonzi Software and UMG Recordings.[350] The FTC brought charges against both corporations under COPPA as well as Section 5 of the FTC Act.[351]

The FTC alleged that both companies failed to obtain verifiable parental consent prior to extensively collecting personal information from children under the age of 13. One of Bonzi's products is the BonziBUDDY, a downloadable software product that interacts with users as they conduct various activities online.[352] As part of registration for the BonziBUDDY, users are required to provide their birth date and other personal information.[353] These birth dates gave

---

[346] UTAH CODE ANN. § 13-39-202.

[347] S.B. 1025, 92 Leg., Reg. Sess. (Mich. 2004).

[348] § 5(1).

[349] H.B. 1809. 2003-2004 Leg. Sess. (Ga. 2004).

[350] Consent Decree, United States v. Bonzi Software, Civ. No. CV-4-1048 RJK (C.D. Cal. filed Feb. 17, 2004) *at* http://www.ftc.gov/os/caselist/bonzi/040217decreebonzi.pdf; Consent Decree, United States v. UMG Recordings, Civ. No. CV-04-1050 JFW (C.D. Cal. filed Feb. 17, 2004)) *at* http://www.ftc.gov/os/caselist/umgrecordings/040217cagumgrecordings.pdf.

[351] *Id.*

[352] Complaint at 4-5, United States v. Bonzi Software, Civ. No. CV-4-1048 RJK (C.D. Cal.) *at* http://www.ftc.gov/os/caselist/bonzi/040217compbonzi.pdf (last visited Feb. 21, 2005).

[353] *Id.*

Bonzi actual knowledge that it was collecting the personal information of children. The FTC alleged that prior to the collection of children's personal information, Bonzi did not obtain verifiable parental consent nor provide notice to parents of the information it sought to collect from children.[354] Additionally, Bonzi allegedly failed to post a clear and conspicuous privacy notice or provide means for parents to review their children's personal information which had been collected.[355]

United States v. UMG Recording is a similar case. UMG operates several general audience websites as well as at least one site specifically directed at children. These websites require registration for participating in activities, resulting in the collection of an array of personal information, including a user's birth date.[356] The collection of the birth date gave UMG actual knowledge that it was collecting personal information from children under the age of 13.[357] The FTC alleged that UMG collected children's personal information without prior notification to and verifiable consent from parents.[358] Although UMG sent notice to some parents after data collection, the lack of prior notification and consent was still in violation of COPPA's parental consent requirement. Additionally, the FTC alleged that in particular instances, personal information was used to market directly to children.[359]

The FTC approved consent decrees regarding both Bonzi and UMG.[360] The decrees require both companies to refrain from committing future violations of COPPA, and to delete any personal information collected from children in violation of COPPA. Additionally, civil penalties and record-keeping requirements were imposed.[361]

---

[354] *Id.* at 5-6.

[355] *Id.*

[356] Complaint at 4-6, United States v. UMG Recordings, Civ. No. CV-04-1050 JFW (C.D. Cal.) *at* http://www.ftc.gov/os/caselist/umgrecordings/040217compumgrecording.pdf (last visited Feb. 21, 2005).

[357] *Id.*

[358] *Id.* at 6-7.

[359] *Id.*

[360] *Supra* note 352.

[361] *Id.*

Three cases at the federal level addressed the constitutionality of statutes protecting children online. Of particular interest, the Supreme Court has upheld a preliminary injunction barring enforcement of COPA.[362] Internet content providers and civil liberties groups argued in federal court that COPA violates the First Amendment.[363] These groups argue that COPA is facially invalid for unduly burdening constitutionally protected adult speech and for violating minors' First Amendment rights. These groups further contend that the statute is unconstitutionally vague.[364] The district court found that in spite of the government's strong interest in protecting children online, the plaintiffs established the likelihood of success on the merits and showing of irreparable harm, and so the court issued a preliminary injunction barring enforcement of COPA.[365] This decision was affirmed by the Third Circuit.[366] Reviewing the district court's decision to grant the preliminary injunction on an abuse of discretion standard, the Supreme Court affirmed the issuance of the preliminary injunction and remanded.[367]

A district court in Pennsylvania has declared unconstitutional a state statute protecting children from pornography.[368] The Internet Child Pornography Act was unique in that it required ISPs to remove or disable access to child pornography items that reside on or are accessible through the ISP's service upon notification by the Pennsylvania Attorney General.[369] Plaintiffs argued that in practice this statute requires ISPs to overblock websites, depriving individuals of accessing innocent content in violation of the First Amendment.[370] They further argue that the statute impermissibly burdens interstate

---

[362] Ashcroft v. ACLU, 124 S.Ct. 2783 (2004).

[363] ACLU v. Reno, 31 F. Supp. 2d 473 (E.D. Pa. 1999).

[364] *Id.* at 477.

[365] *Id.* at 497-98.

[366] ACLU v. Reno, 217 F.3d 162 (3d Cir. 2000).

[367] Ashcroft v. ACLU, 124 S.Ct. at 2785-86.

[368] Center for Democracy & Technology v. Pappert, 337 F. Supp. 2d. 606 (E.D. Pa. 2004).

[369] 18 PA. CONS. STAT. § 7622.

[370] CDT v. Pappert, 337 F.Supp. 2d. at 611.

commerce in violation of the dormant Commerce Clause.[371] The Court found that in practice, the statutorily required filtering by the ISPs resulted in the blocking of legitimate content.[372] This filtering unduly burdens speech in violation of the First Amendment.[373] The Court further found that the "Act's extraterritorial effect violates the dormant Commerce Clause."[374] For these reasons, the statute was declared unconstitutional.

The Fourth Circuit denied a petition regarding a lower court decision that declared a Virginia state law protecting minors from access to Internet pornography unconstitutional.[375] Of the thirteen active judges on the Circuit, eight disqualified themselves from participation in Virginia's request for a rehearing *en banc* of a 2-1 decision declaring the state law unconstitutional.[376] Virginia had amended a state law to make it a crime to use the Internet to sell, rent, or lend pictures which depict sexual excitement, conduct, or sadomasochistic abuse that may be harmful to juveniles.[377] PSINet and others argued in federal court that the amendment was overly broad in that it would deny access to many educational websites on the web and deprive adults and minors of useful information. While acknowledging that protecting minors from exposure to sexually explicit materials is a valid state interest, the district court judge found the statute was overbroad and infringed on adults' free speech rights.[378]

D. STATE LITIGATION

State litigation also addressed the constitutionality of a statute pertaining to the protection of children from Internet pornography. A

---

[371] *Id.*

[372] *Id.* at 633-34, 637-42.

[373] *Id.* at 652, 656, 658.

[374] *Id.* at 663.

[375] PSINet Inc. v. Chapman, 372 F.3d 671 (4th Cir. 2004).

[376] *Eight Recusals Lead to Denial of Rehearing in Va. Internet Case*, 8 No. 4 Andrews Litig. Rep. 5, July 15, 2004.

[377] *Id.*

[378] *Id.*

state appeals court in Florida upheld the constitutionality of a Florida statute aimed at protecting children from pornography.[379] The appellant pled *nolo contendere* to a violation of the Computer Pornography and Child Exploitation Prevention Act, which specifically prohibits the knowing utilization of the Internet to seduce, solicit, or entice a child to commit an illegal act relating to sexual battery, lewdness or indecent exposure, or child abuse.[380] The appellant argued that the Act is unconstitutional in that it functions as a content-based restriction on pure speech and is violative of the dormant Commerce Clause.[381] The court found these arguments to be without merit and upheld the constitutionality of the statute.

E. CONCLUSION

Child online protection has been less of a hot button issue than spam, spyware, and fraud. That said, legislation was introduced at the federal and state level, and the FTC brought action under federal child protection laws. The focus of litigation regarding child protection statutes has not been enforcement, but rather the statutes' viability. There appears to be a trend towards challenging the constitutionality of both state and federal statutes. Continued monitoring is required to assess the status of these challenged statutes.

X. CONCLUSION

The eight topics discussed – spyware, spam, phishing & spoofing, Internet governance, fraud & wrongdoing, contemporaneous monitoring of Internet activity, access to stored records from Internet activity, and, finally, online protection for children – represent a substantial amount of the activity relating to the Internet and privacy in 2004. Many of these topics deal with complex issues that remain unresolved, which all but guarantees continued interest in 2005 and beyond.

---

[379] Cashatt v. Florida, 873 So.2d 430 (Ct. App. Fla. April 26, 2004) (per curiam).

[380] FLA. STAT. ch. 847.0135(3).

[381] *Cashatt*, 873 So.2d at 434.